ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИРКУТСКОЙ ОБЛАСТИ «БРАТСКИЙ ПРОМЫШЛЕННЫЙ ТЕХНИКУМ»

КОМПЛЕКТ МЕТОДИЧЕСКИХ УКАЗАНИЙ

по выполнению практических работ
ПО ПРОФЕССИОНАЛЬНМУ МОДУЛЮ
ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ

по теме:
«Основы цифровой и компьютерной безопасности»

230401. Информационные системы (в строительстве)

Братск, 2015

Методическое пособие по выполнению практических работ разработано в соответствии с рабочей программой профессионального модуля «Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих», требованиями ФГОС СПО и адресованы студентам по специальности среднего профессионального образования 230401 *Информационные системы (в строительстве)*

Организация: Государственное бюджетное профессиональное образовательное учреждение Иркутской области «Братский промышленный техникум»

Автор-составитель:

Петрович А. В., преподаватель информационных дисциплин

Рецензент:

Методические указания одобрены на заседании цикловой комиссии

Протокол №_____ от «_____» _____ 20___ г.

Председатель ЦК _____ /Орлова Н.А./

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии — ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому подтверждение.

Криптографическое закрытие является специфическим способом защиты информации, оно имеет многовековую историю развития и применения. Поэтому у специалистов не возникло сомнений в том, что эти средства могут эффективно использоваться также и для защиты информации в автоматизированных системах обработки данных, вследствие чего им уделялось и продолжает уделяться большое внимание.

В данном методическом указании кратко изложены теоретические основы двух криптографических методов относящихся к шифрованию заменой или подстановкой (схема шифрования Вижинера, шифр Цезаря), приведены примеры выполнения шифрования и дешифрования сообщений с помощью указанных методов, даны указания по выполнению практической работы и задания для самостоятельного выполнения (по вариантам).

Мы живем на стыке двух тысячелетий, когда человечество вступило в эпоху новой научно-технической революции. К концу двадцатого века люди овладели многими тайнами превращения вещества и энергии и сумели использовать эти знания для улучшения своей жизни. Но кроме вещества и энергии в жизни человека огромную роль играет еще одна составляющая - информация. В связи со стремительным развитием информационных технологий и их проникновением во все сферы человеческой деятельности возросло количество преступлений, направленных против информационной безопасности.

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

С каждым днем вирусы становятся все более изощренными, что приводит к существенному изменению профиля угроз. Но и рынок антивирусного программного обеспечения не стоит на месте, предлагая множество разнообразных антивирусных продуктов.

В данном методическом указании кратко изложены теоретические основы понятия вируса, виды вирусов, виды антивирусных программ, приведен примеры выполнения антивирусной защиты компьютера, даны указания по выполнению практической работы.

ПРАКТИЧЕСКАЯ РАБОТА «АНАЛИЗ И СРАВНЕНИЕ ВОЗМОЖНОСТЕЙ АНТИВИРУСНЫХ ПРОГРАММ»

Цель работы: ознакомиться с теоретической частью защиты информации от вредоносных программ: разновидностью вирусов, способов заражения и методов борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Получить навыки работы с антивирусной программой Антивирус Касперского и другими.

Краткие теоретические сведения:

Понятие компьютерного вируса

Среди огромного разнообразия видов компьютерных программ существует одна их разновидность, которая представляет опасность для ЭВМ. Это - компьютерные вирусы.

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или файловую систему диска, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющихся в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Происхождение компьютерных вирусов

Компьютерные вирусы создаются такими же (а иногда и теми же) людьми, что пишут самые обычные программы. Кто-то со зла на все человечество или на значительную его часть рассматривает вирусы как разновидность бомбы, которую легко создать и трудно проследить до первоисточника. Но среди авторов вирусов встречаются и высококвалифицированные программисты, люди образованные, корректные, психически устойчивые.

К сожалению, именно их трудами технология «вирусописательства» движется вперед. Для них исследование и разработка вирусов - это поле для творчества и средство для самовыражения. Такие авторы не создают разрушительные вирусы, но придумывают новые механизмы их размножения и распространения. Но на каждого «научного» исследователя приходится несколько сот менее щепетильных людей. Как следствие, самый «теоретический» вирус вскоре проявляется в разрушительной практической ипостаси.

На сегодняшний день число различных компьютерных вирусов измеряется тысячами, так что возникла необходимость их классификации. Основным принципом такой классификации сегодня является место размещения вируса в компьютерной системе. В отличие от разрушительного эффекта (который может быть любым) разнообразие мест размещения вирусов и связанных с этим способов их распространения невелико. Новые методы появляются редко и обычно связаны с появлением новых средств связи или новых принципов работы программного обеспечения.

При классификации вирусов по месту размещения трудности вызывают только вирусы комплексной природы, использующие для распространения несколько разных механизмов. Такие вирусы отличаются повышенной эффективностью распространения, но в этом случае и не

слишком опытному пользователю легко заметить, что на его компьютере происходит что-тонеобычное.

Классификация вирусов
Троянские кони и логические бомбы

Компьютерные вирусы берут свое начало от этих двух типов враждебных программ.

Типичный «троянец» скрытно работает на компьютере жертвы, позволяя брать его под удаленное управление через Интернет. У программ этого рода отсутствуют средства самовоспроизведения (автоматического распространения). Они маскируются под полезную программу или присоединяются к таковой злоумышленником. Таким образом, характерной особенностью троянской программы является несоответствие явных и скрытых функций.

Разделение на троянские программы и логические бомбы условно. Под собственно троянскими программами обычно понимают программы, ориентированные на долговременное скрытное исполнение паразитных функций. Логическая бомба обычно должна сработать один раз, но с максимальной разрушительной силой. В нормальных условиях она пассивна, и поэтому пользователь не подозревает о ее присутствии. При возникновении условий активации, которые не обязательно имеют природу команды, бомба «взрывается». Последствия срабатывания бомбы могут быть любыми.

С формальной точки зрения, троянские кони и логические бомбы не являются вирусами, так как не имеют средств самовоспроизведения. Но они, без сомнения, принадлежат к общей группе враждебных программ. Антивирусные программы регистрируют наличие на компьютере любых враждебных программ как «заражение».

Загрузочные вирусы

Программный код, в том числе и вирусный, может нести даже пустой диск, потому что любой дисковый носитель имеет служебную область, называемую загрузочным сектором. При попытке загрузки с диска процессор обращается к коду, имеющемуся в этом секторе. Если диск не является загрузочным, то такой код лишь выдает на экран предупреждающее сообщение и дает возможность повторить попытку загрузки.

Загрузочный вирус подменяет или расширяет этот код. При обращении к зараженному диску сначала происходит загрузка в оперативную память враждебного кода и только потом запускается код истинной загрузочной записи.

Гибкий диск может не быть системным и не предназначаться для загрузки операционной системы. Но и в этом случае при попытке загрузки с зараженной дискеты код вируса проникает в память и заражает загрузочную область системного жесткого диска. Далее вирус активизируется при каждом запуске компьютера и поражает загрузочные области всех обнаруженных дисков, не защищенных от записи.

Распространение загрузочных вирусов происходит благодаря переносу зараженных гибких дисков между компьютерами руками самих пользователей.

Для защиты от загрузочных вирусов в параметрах настройки BIOS отключают возможность загрузки компьютера с гибкого диска A, CD дисков и USB носителей. Излечение зараженных служебных секторов жестких дисков обычно не представляет серьезных проблем, если не наступила стадия разрушительных действий. Диски эффективно излечиваются путем полного переформатирования. Перед этим данные можно переписать на любой другой носитель, в том числе и на жесткий диск. При копировании файлов загрузочные вирусы не переносятся - они требуют попытки загрузки операционной системы с данного носителя.

Файловые вирусы

Вирусы, дописывающие свой код к файлам, называются файловыми. Они поступают в оперативную память при запуске пораженного файла. Источники таких вирусов - исполнимые файлы, то есть файлы программ (*.COM и *.EXE), а также файлы программных библиотек, например *.DLL.

Вирус активизируется при запуске зараженного файла. Дальнейшее его поведение может быть разным. Некоторые вирусы сами разыскивают файлы на жестком диске и заражают их, другие остаются в памяти как резидентные программы и заражают все файлы, запущенные после активизации вируса.

Стелс-вирусы

Стелс-технология(stealth) используется для скрытия факта присутствия файлового вируса от антивирусных программ. Принцип действия состоит в том, что вирус перехватывает обращения антивирусной программы, разыскивающей характерные фрагменты кода, и предоставляет ей текст незараженного файла.

Современные антивирусные программы успешно борются с этой категорией вирусов-невидимок. Выявить истинную картину позволяет выполнение операции чтения в обход стандартных средств операционной системы.

Полиморфные вирусы

Полиморфные вирусы пытаются ввести в заблуждение антивирусные средства, уходя от повторяющихся сигнатур. Для этого они шифруют собственный код с

помощью случайного ключа, который, как правило, берется из заражаемого файла. Расшифровка кода вируса производится динамически, во время его работы.

Видимый код вируса непредсказуем, и сличать его с образцами известных вирусов бессмысленно. Для обнаружения полиморфных вирусов требуется эвристический анализ кода. Сам факт шифрования кода уже является подозрительным признаком.

Макровирусы

Долгое время считалось, что вирусы способны поражать только объекты, содержащие исполнимый код (файлы и загрузочные области носителей), но никак не объекты, в которых хранятся данные: документы, сообщения, записи баз данных.

Однако вирусы такого типа сегодня более «популярны», чем файловые вирусы, поражающие исполняемые файлы.

В операционной системе Windows активно используются объекты серверного типа, способные исполнять команды, хранимые в документах (файлах данных). В этом случае документ, содержащий данные, способен запускать несанкционированные процессы. При этом сам документ не является исполнителем этих процессов. Все действия выполняет иная программа, ранее установленная на компьютере и заведомо не являющаяся враждебной. Вредоносный «вирусный» компонент связан не с программой, а именно с документом.

Документы, созданные средствами пакета Microsoft Office и OpenOffice, могут содержать так называемые макросы, в основе которых лежит язык программирования Visual Basic for Applications (VBA). Сценарии VBA включаются в состав документа и работают под управлением родительского приложения. Существуют средства автоматического запуска сценариев при активизации документа, что и позволяет макросам иметь вирусное содержание.

Сомнительной популярности макровирусов способствует простота их создания и отсутствие привязки к конкретной платформе. Кроме того, передача документов происходит гораздо чаще, чем передача программных файлов. Многие документы, например, в формате Word, с самого начала разрабатываются для последующей передачи. Это очень «удобно» для распространения заразы.

Защита от макровирусов

Защита от макровирусов бывает активной и пассивной. Активная защита предполагает регулярную проверку компьютера с помощью антивирусных программ и обязательную проверку документов, поступающих извне. Пассивная защита основана на настройке системы защиты средствами Microsoft Office, OpenOffice и добровольных самоограничениях. Не вдаваясь в подробности, стоит отметить, что предложенная система неудобна, трудоемка и малоэффективна. Применение специальных антивирусных средств дает лучший эффект.

Сетевые и почтовые вирусы

Особую категорию составляют сетевые и почтовые вирусы, средой обитания которых являются компьютерные сети. Теоретически, такие вирусы могут вообще не сохраняться на носителях данных, а пребывать в оперативной памяти или находиться в процессе пересылки с одного компьютера на другой. Большие компьютерные сети работают в режиме постоянной эксплуатации, так что гибель

подобного вируса в связи с выключением всех компьютеров, на которых он «завелся», маловероятна.

Сетевые вирусы, или сетевые черви, используют уязвимости компьютерных сетей, чтобы передать свой код на другой компьютер и создать на нем новый рабочий процесс, исполняющий червя. Это технически сложная процедура, требующая высокой квалификации автора программы, почему сетевые черви встречаются достаточно редко. Они ориентированы на поражение серверных систем и не опасны для домашних или офисных рабочих станций.

Гораздо менее «приятна» такая разновидность сетевых вирусов, как почтовые вирусы.

Они распространяются вместе с сообщениями электронной почты. Технический прогресс вытеснил из оборота гибкие магнитные диски, с уходом которых активность загрузочных и файловых вирусов снизилась. Их место успешно заняли вирусы почтовые, распространяющиеся через Интернет. Сегодня это один из наиболее распространенных типов компьютерных вирусов.

Механизм распространения почтовых вирусов основан на сканировании адресной книги клиентского компьютера и дальнейшей рассылки сообщения от имени жертвы. Фактически, рассылка сообщений («размножение вируса») происходит немедленно после его попадания на компьютер, так что к вредоносным действиям, если такие предусмотрены, вирус также может приступать немедленно.

Существует несколько механизмов распространения вирусов в почтовых сообщениях:

- файловый;
- сценарный;
- на основе HTML.

В первом случае вирус эксплуатирует неосведомленность или беспечность пользователя, во втором - серверные свойства операционной системы клиентского компьютера, а в третьем - ошибки коммуникационных программ, в первую очередь

Internet Explorer, Microsoft Outlook или Outlook Express.

Файловый механизм распространения

В этом случае почтовое сообщение содержит присоединенный файл, зараженный файловым вирусом. Поражение компьютера происходит при запуске этого файла, который жертва должна выполнить собственноручно. Ее убеждают сделать это методами социальной инженерии. В тексте сообщения автор послания доходчиво объясняет, как важно запустить присоединенный файл, и убедительно рекомендует распространить его среди друзей и знакомых.

Для распространения вирусов нередко используется именно страх перед вирусами. Всевозможные «предупреждения» и «лечебные средства», поступившие от «доброжелателей» (или даже от знакомых), практически гарантированно содержат не лекарство, а возбудитель болезни.

Для защиты от подобных вирусов следует придерживаться простейших правил.

1. Не рассылайте по электронной почте вложенные файлы иначе как по прямой просьбе партнера. Если файл надо отправить без предварительного согласования, сообщение должно содержать подробное описание приложенного файла и изложение причин, по которым он отправлен.
2. Не присоединяйте исполнимые файлы к сообщениям электронной почты. Если это сделать необходимо, файл следует предварительно запаковать архивирующей программой. Не следует создавать и пересылать самораспаковывающиеся архивы.
3. Никогда не рассылайте и не пересылайте сообщения, которые предлагается далее направить «всем друзьям и знакомым», независимо от того, содержат они вложения или нет.

4. При получении незатребованного сообщения электронной почты, содержащего вложенные исполнимые файлы, удалите его, не взирая на имя отправителя. При наличии сомнений отложите присланное вложение в отдельную папку и направьте отправителю дополнительный запрос-уточнение.

Сценарный механизм распространения

Знающий человек вряд ли запустит неизвестную программу, но почтовых вирусов от этого меньше не стало. Активно распространяются сценарные почтовые вирусы, для запуска которых не надо извлекать и запускать исполнимый файл - достаточно просто щелкнуть на значке почтового вложения.

Этот тип вируса оказался невероятно живучим - количество его клонов и разновидностей исчисляется многими сотнями. Технология создания вирусов этого типа исключительно проста, имеются специальные программы-генераторы. «Творцу» такого вируса остается только придумать громкое имя.

Механизм работы сценарных почтовых вирусов основан на использовании сервера сценариев Windows Scripting Host (WSH) и языка программирования VBScript (не путать с Visual Basic и Visual Basic for Applications) или JScript (не путать с JavaScript).

На каждом компьютере с операционной системой Windows по умолчанию работает так называемый сервер сценариев, который позволяет исполнять последовательности команд, записанных в текстовых файлах с расширением имени VBS, .JS и некоторых других.

В сценарных языках VBScript u JScript нет прямых команд для изменения данных на жестком диске, но, к сожалению, это не значит, что они безопасны. С их помощью можно создать в памяти компьютера экземпляры объектов, для которых у сервера WSH имеются заготовки. Эти объекты уже могут создавать файлы и папки, записывать в них все что угодно, удалять то, что не нравится, контролировать компьютер и локальную сеть, к которой он принадлежит.

Злоумышленник пишет текстовый файл, содержащий команды языка VBScript для создания в памяти компьютера вредоносного объекта и управления им. Далее этот файл сохраняется с расширением .VBS и прикладывается к сообщению электронной почты в виде почтового вложения. Чтобы невнимательный пользователь не обратил внимания на расширение имени, название файла записывается «по-хитрому, например, *I love you.TXT.vbs* или, например, *Anna Kournikova.JPG.vbs*. Когда в имени файла присутствует несколько точек, расширением имени считаются символы, расположенные правее последней точки. Не все почтовые клиенты отображают расширение имени, да и пользователи не всегда внимательны. Многие из них приняли вложенный файл *I love you.TXT.vbs* за обычный текст, а файл *Anna Kournikova.JPG.vbs* за фотографию известной спортсменки, после чего дали команду открыть вложение и тем самым запустили сервер WHS на исполнение враждебного кода.

Со сценарными вирусами борются примерно так же, как с файловыми. Аккуратность и осмотрительность при работе с сообщениями электронной почты, содержащими вложенные файлы, остается важным фактором безопасности. Не следует доверять даже родным и близким - почтовый вирус чаще всего присылает сообщение от имени знакомого, из чьей адресной книги он смог позаимствовать адрес.

Верно решить судьбу поступившего файла в сложных ситуациях помогут антивирусные программы. Можно также полностью отключить сервер сценариев WSH, удалив или переименовав файл C:\Windows\wscript.exe.

Распространение вирусов с использованием HTML

В языке HTML, используемом для описания Web-страниц, по самому замыслу нет и не может быть команд, способных повредить читателю. Однако сочетание различных средств, по отдельности безобидных, способно привести к весьма неприятным эффектам.

Язык HTML (точнее, особенности его реализации в продуктах компании Microsoft) дал возможность активизировать вирусы, присоединенные к почтовому сообщению, уже при его просмотре, то есть без прямого обращения к вложению.

Принцип такой активизации основан на том, что современные сообщения электронной почты могут содержать текст, оформленный средствами HTML, - форматированный текст со вставными объектами (например, музыкой и графикой). При работе в почтовых программах Microsoft Outlook, Outlook Express и других формат сообщения выбирается его автором. В частности, в почтовом клиенте Outlook Express формат исходящих сообщений выбирается на вкладке Отправка сообщений диалогового окна Параметры (Сервис → Параметры). Там же можно и настроить некоторые параметры программы, связанные с пересылкой кода HTML.

При приеме сообщений возможность управления форматом отсутствует. Например, в программах Outlook и Outlook Express нет настройки, которая позволила бы удалить из сообщения коды HTML или вообще отказаться от приема сообщений в таком формате. Если входящее сообщение имеет формат HTML, почтовая программа привлекает для его отображения средства Internet Explorer. В этом и состоит уязвимость.

Используя дефекты программы Internet Explorer, почтовое сообщение может активизировать файл вложения при просмотре сообщения или инициировать запуск вирусного кода при перезагрузке компьютера. В любом случае вирус активизируется без привлечения пользователя.

Бороться с подобными вирусами можно по-разному.

1. Не пользоваться коммуникационными программами компании Microsoft, чтобы исключить специфические уязвимости Outlook Express и Internet Explorer. Это предупредит проникновение на компьютер многих «модных» вирусов, но такой прием ни в коем случае нельзя считать панацеей — другие программы также небезгрешны и уязвимы.
2. Пользоваться проверенными антивирусными средствами. Они не всегда защитят от вирусов, автоматически запускающихся при просмотре электронных писем, но по крайней мере предупредят об уязвимостях в системе безопасности операционной системы, браузера или почтового клиента и порекомендуют приемы их устранения.
3. Не спешить просматривать полученные сообщения. Сначала просмотрите поступившие заголовки. Если среди сообщений есть подозрительные (из незнакомых источников или со странными темами), не открывайте их, а вместо этого щелкните на заголовке сообщения правой кнопкой мыши и в контекстном меню выберите пункт Удалить.

Удаление сообщения не означает его утраты. По команде удаления оно перемещается в папку Удаленные, где его можно впоследствии прочитать, если подозрения окажутся безосновательными.

От распространения почтовых вирусов иногда помогает простое «народное» средство. Создайте в адресной книге (в списке контактов) пару липовых записей, не содержащих адреса. Одну запись добавляем в начало списка контактов («корреспондент» аааaa - буквы английские), а вторую запись - в конец списка (яяяяя). Если на компьютер проникнет почтовый вирус и попытается разослать свои копии, он «споткнется» о фальшивый контакт и рассылки не произойдет.

Если при создании нового контакта в программе Outlook Express кнопка Добавить не работает, пока не введен адрес электронной почты, не обращайте на это внимания: нажмите кнопку ОК - этого достаточно, чтобы создать запись.

Антивирусные программы и пакеты

Вскоре после появления первых вирусов были созданы противостоящие им антивирусные средства. Компьютерные вирусы непрерывно совершенствуются. То же происходит и с антивирусными средствами. Сегодня защитные функции уже не возлагаются на единичную антивирусную программу. Пакеты антивирусных программ состоят из нескольких компонентов, каждый из которых решает свою задачу.

Термин «антивирус» носит исторический характер. Как уже упоминалось, антивирусные пакеты предназначены для борьбы со всеми типами враждебных программ.

В частности, механизмы объединения двух программ в один исполняемый файл рассматриваются как средство внедрения троянских программ и вызывают реакцию со стороны антивирусных средств.

Сканирующие программы

Сканеры просматривают оперативную память компьютера и носители данных (служебные секторы и файловую структуру) в поисках вирусоподобных объектов.

Поиск вирусов основан на сличении фрагментов кода или иных признаков с образцами, характерными для известных вирусов, зарегистрированных в антивирусной базе данных. Современные антивирусные сканеры способны выявить и самошифрующиеся (полиморфные) вирусы.

Кроме розыска вирусов, сканеры выполняют и лечебно-предохранительные функции. Они обычно способны уничтожить вирус и восстановить исходное состояние файла. Файл также можно переименовать, удалить или отправить в «карантин» - специальную папку, исключающую активизацию вируса. При «лечении» зараженных файлов сохраняется опасность их необратимого повреждения, поэтому для ценных файлов принято перед лечением создавать в карантинной папке копию.

Если антивирусная программа не поддерживает работу с карантинной папкой, можно организовать карантин своими руками. Для этого достаточно запаковать подозрительный файл каким-либо архиватором и сохранить архив в надежном месте. Вирус, содержащийся в заархивированном файле, работать не может.

Хорошие антивирусные сканеры обладают и дополнительными функциями: возможностью запуска с гибкого диска, средствами поиска вирусов в архивах, базах данных и запакованных файлах. Полезны также средства интеграции с Проводником Windows. В последнем случае запустить сканирование можно через контекстное меню. Это удобно, если надо проверить отдельный объект (файл или папку).

Антивирусные мониторы

Мониторами называют средства наблюдения за идущими процессами. Соответственно, антивирусные мониторы - это программы, работающие в фоновом режиме и наблюдающие за файловыми операциями операционной системы (копирование, открытие, запуск и другие). Антивирусный монитор можно считать сканером, работающим в режиме реального времени. Сканер запускается по желанию, например, один раз в месяц, а монитор работает всегда. Он включается при загрузке компьютера и следит за всеми операциями.

Между сканерами и мониторами есть большая разница. Цель сканера - обнаружить вирусы, имеющиеся на компьютере. Цель монитора - поймать вирус при попытке проникновения.

Например, на компьютере можно установить несколько сканеров разных производителей. В этом случае сильные стороны одного сканера могут компенсировать слабости другого. Устанавливать несколько мониторов не имеет смысла - они выполняют одни и те же операции в одно и то же время и могут только мешать друг другу. Эффективность и устойчивость работы компьютера почти наверняка упадут.

Программы-ревизоры

Ревизоры, или инспекторы, встречаются в самых серьезных версиях антивирусных пакетов, рассчитанных на корпоративного или профессионального потребителя.

Основная задача ревизора - контролировать вирусную активность, то есть регистрировать вирусные или вирусоподобные действия. Ревизор способен обнаружить даже неизвестные вирусы, сведения о которых отсутствуют в антивирусной базе данных.

Программа-ревизор отслеживает изменение файлов, хранящихся на дисках, а также служебных записей диска. При первом запуске создается база данных, в которую записываются размеры и контрольные суммы файлов, а также их атрибуты и некоторые другие данные. Для наиболее важных системных файлов этих данных достаточно, чтобы восстановить файл в случае повреждения. Кроме того, ревизор сохраняет дубликаты служебных разделов дисков (глав-

ная загрузочная запись, загрузочные записи дисков, содержимое корневого каталога), чтобы и в случае катастрофы пользователь мог добраться до своих файлов.
При последующих запусках (или в фоновом режиме работы) ревизор проверяет эти данные для зарегистрированных файлов. Десятки и сотни файлов создаются и модифицируются на компьютере ежедневно, что ни в коей мере не говорит о деятельности вирусов. Но некоторые изменения дают основание для подозрений – и о них ревизор сигнализирует. Вот какие изменения считаются подозрительными:

- изменено содержимое файла, а дата создания или последнего изменения файла не изменилась;
- размеры разных файлов изменились одинаково;
- в атрибутах файла появилась некорректная дата или время, что может быть пометкой, сделанной файловым вирусом;
- изменен важный системный файл, внесенный в список файлов, не подлежащих изменению.

Принципы действия программ-ревизоров хорошо известны создателям вирусов. Поэтому нередко вирус начинает работу с того, что пытается обнаружить и заглушить программу-ревизор, чтобы она не могла сообщить о подозрительной
деятельности.

Средства автоматического обновления антивирусных баз

В основе всех программных продуктов антивирусного пакета лежат антивирусные базы данных. Регулярное появление новых вирусов и их разновидностей требует столь же регулярного обновления этих баз. Разработчики антивирусных средств выкладывают дополнения к базам на своих сайтах ежедневно, так как для некоторых почтовых вирусов возникновение и развитие «эпидемии» происходит буквально за несколько часов. Но частоту обновления своих баз выбирает пользователь - он может избрать ежедневное, еженедельное, ежемесячное или кумулятивное обновление. В последнем случае базы приводятся в актуальное состояние независимо от даты предыдущего обновления.

Кумулятивное обновление можно выполнять вручную, время от времени (не обязательно регулярно) посещая Web-узел разработчика. Но регулярные обновления целесообразно автоматизировать. Для этого в состав пакета обычно входит специальный модуль, способный автоматически связаться с сайтом поставщика антивирусных баз, принять необходимые файлы и обновить действующую базу.

Комплекты аварийного восстановления

Хорошее антивирусное средство предусматривает возможность того, что его попытаются применить слишком поздно - тогда, когда вирус уже успел начать свою разрушительную деятельность и, возможно, вывести из строя жесткий диск. На такой случай можно создать комплект дисков, с помощью которых можно проверить компьютер на наличие вирусов даже при неработающем жестком диске.

Во многих случаях удается не только установить наличие вируса, но и ликвидировать его последствия, хотя бы самые критичные, препятствующие нормальному запуску.

Планировщики заданий

Недостаток антивирусной системы состоит в том, что постоянный антивирусный контроль заметно снижает эффективность работы. При нормально организованной работе угроза заражения не столь уж высока, и желательно организовать работу антивирусных средств так, чтобы они не превращались в помеху.

Например, достаточно, если сканер отработает один раз в сутки - утром или вечером. Но, например, мониторы и ревизоры эффективны, только если они работают постоянно, запускаясь вместе с операционной системой. Средства обновления баз данных можно запускать - раз в день или в неделю.

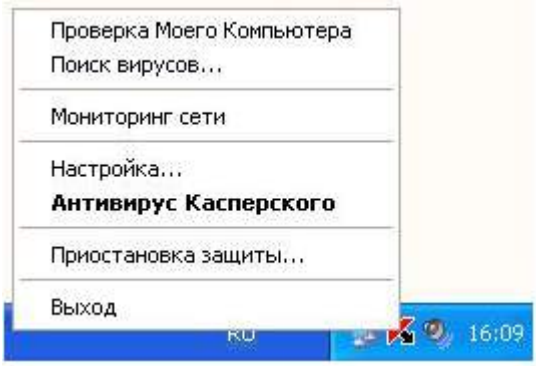
Организовать запуск нужных программ по приемлемому расписанию позволяют специальные программы, планировщики заданий, цель которых – автоматизация рутинных операций. Настроив планировщик один раз, можно навсегда забыть о компьютерных вирусах и доверить борьбу с ними автоматике и поставщику антивирусных средств.

Задание № 1

1. Убедитесь в том что, Антивирус Касперского в данный момент загружен и работает, об этом символизирует иконка на системной панели в правом нижнем углу экрана. В зависимости от задачи, выполняемой антивирусом, картинка на ней может меняться. В дальнейшем в ходе лабораторных работ во время выполнения разных задач всегда обращайте внимание на вид этой иконки.

Дополнительно она служит для быстрого доступа к основным функциям антивируса: двойной щелчок левой клавишей мыши на ней вызывает главное окно интерфейса, а контекстное меню, открываемое щелчком правой клавиши мыши позволяет сразу перейти на нужное окно интерфейса.

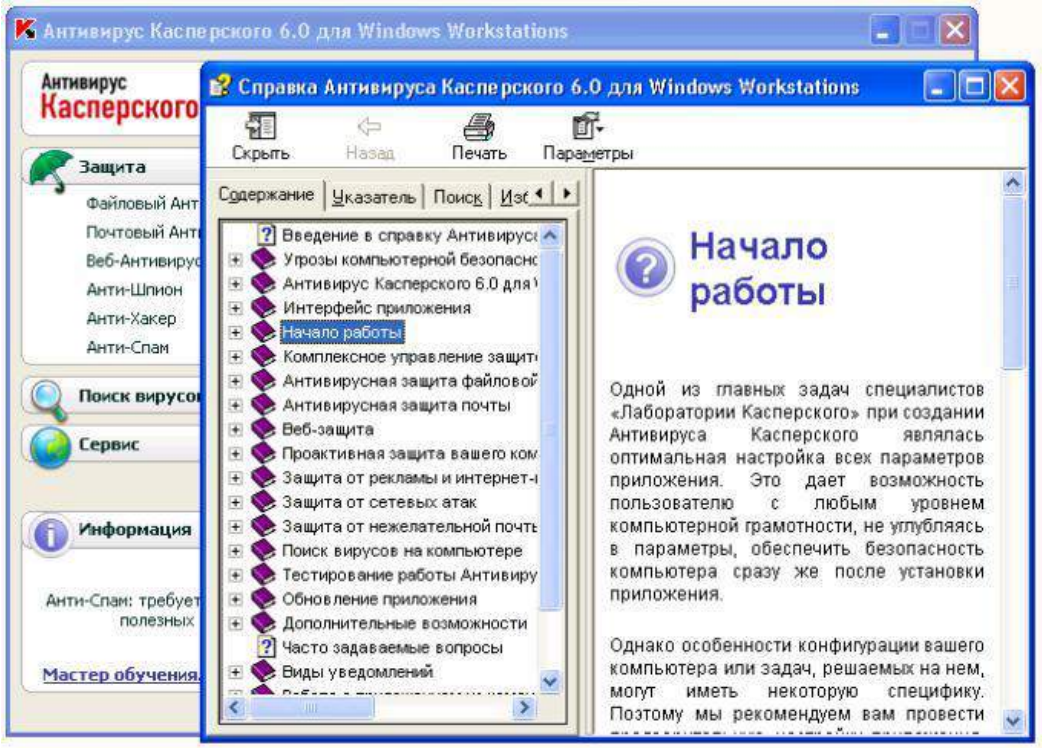
Откройте контекстное меню иконки Антивируса Касперского и ознакомьтесь с представленным здесь списком ссылок:



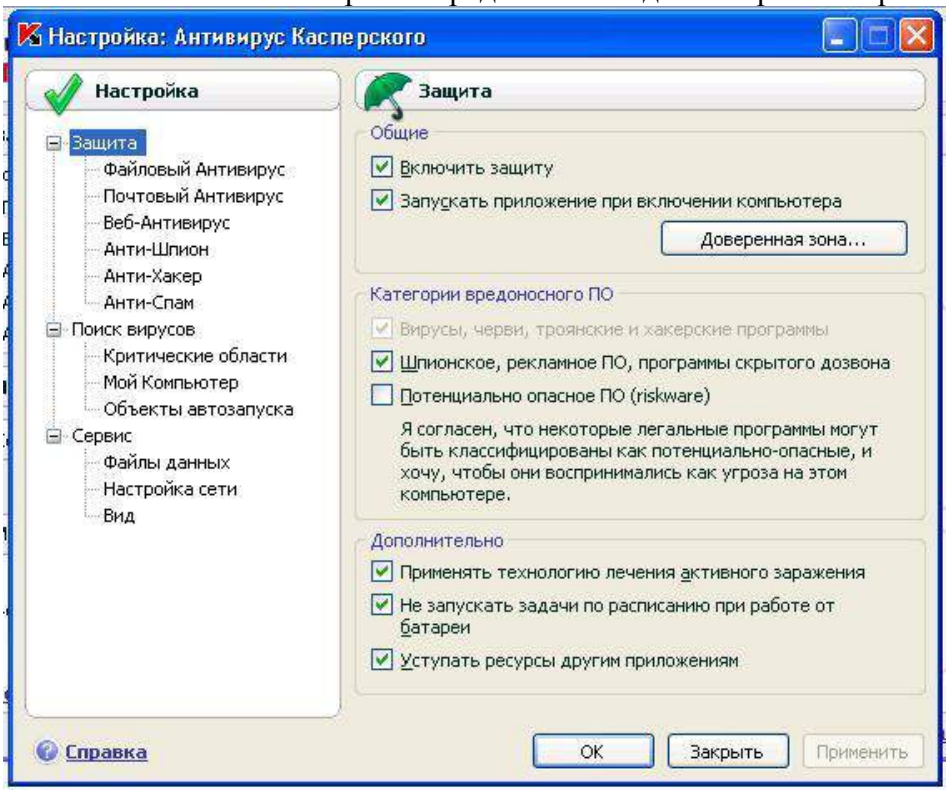
2. С помощью двойного щелчка на иконке откройте главное окно интерфейса Антивируса Касперского:

3. В верхней правой части окна размещено две ссылки: Настройка и Справка. Первая используется для настройки антивируса, вторая - для вывода справочной системы.

Нажмите ссылку Справка Открывшееся окно содержит руководство пользователя Антивирусом Касперского. При возникновении каких-либо проблем, в первую очередь всегда нужно обращаться к нему. Ознакомьтесь с содержанием справочной системы в левой панели окна и закрыв его вернитесь к главному окну антивируса



4. В главном окне нажмите ссылку Настройка, расположенную слева от Справка. Открывшееся окно Настройка предназначено для настройки параметров работы антивируса.



5. Изучите настройки антивируса. Какие по вашему мнению для эффективной работы антивируса лучше произвести настройки?

По интересующим вопросам обратитесь к разделу Справка. Сохраните ваши настройки.

6. Зайдите в раздел поиска вирусов нажав на кнопку в контекстном меню

. Произведите выбор объектов для проверки нажав на кнопку «Добавить» и «Удалить». Произведите поиск вирусов нажав на кнопку «Поиск вирусов».

7. При окончании поиска изучите файл отчета поиска.

Задание № 2

1. Чтобы проверить насколько эффективно работает антивирус создайте текстовый файл.
2. В текстовый файл вставьте строку с кодом вируса.

*X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H**

Сохраните файл.

Если вы произвели правильные настройки антивируса, то он мгновенно должен отреагировать на созданный вами файл.

Задание № 3

1. Откройте ваш текстовый процессор.
2. Произведите настройки вашего текстового процессора от макровирусов установив высокую степень защиты. Для этого зайдите в Параметры→Безопасность.

Задание № 4

Подготовьте доклад и презентацию на тему: «Общие сведения и особенности работы антивирусной программы *[Название антивирусной программы]*». Название антивирусной программы выбрать согласно своему варианту из вариантов заданий к работе.

Объем доклада 4-5страницы. Слайдов в презентации не менее пяти, по времени7-10минут.

Варианты заданий:

Вариант	Название антивирусной программы
1	AVG
2	Dr.Web
3	Avira
4	Panda AntiVirus
5	McAfee VirusScan
6	Eset Nod32
7	Microsoft Security Essentials
8	Norton AntiVirus
9	Антивирус Касперского
10	Avast!

ПРАКТИЧЕСКАЯ РАБОТА
«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Цель работы: познакомиться с криптографическими методами преобразования информации. Научиться выполнять шифрование и дешифрование сообщений с помощью шифра Цезаря и с помощью подматриц Вижинера.

Краткие теоретические сведения

Шифр Цезаря

Историческим примером шифра замены является шифр Цезаря (1 век до н.э.), описанный историком Древнего Рима Светонием. Гай Юлий Цезарь использовал в своей переписке шифр собственного изобретения. Применительно к современному русскому языку он состоял в следующем. Выписывался алфавит: А, Б, В, Г, Д, Е,… затем под ним выписывался тот же алфавит, но со сдвигом на 3 буквы влево:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В

Рис 1. Таблица для шифра Цезаря

При зашифровке буква А заменялась буквой Г, Б заменялась на Д и так далее. Так, например, слово "РИМ" превращалось в слово "УЛП". Получатель сообщения "УЛП" искал эти буквы в нижней строке и по буквам над ними восстанавливал исходное слово "РИМ". Ключом в шифре Цезаря является величина сдвига 3-й нижней строки алфавита (рис. 1). Преемник Юлия Цезаря — Цезарь Август — использовал тот же шифр, но с ключом — сдвиг 4. Слово "РИМ" он в этом случае зашифровал бы в буквосочетание "ФМР".

Для шифра Цезаря имеется более простой способ расшифровки — так называемый метод полосок. На каждую полоску наносятся по порядку все буквы алфавита. В криптограмме берется некоторое слово. Полоски прикладываются друг к другу так, чтобы образовать данное слово. Двигаясь вдоль полосок находится осмысленное словосочетание, которое и служит расшифровкой данного слова, одновременно находится и величина сдвига.

На рисунке 2 видно, что под выделенной строкой сложенной шифрограммы можно прочитать слово полезен. Таким образом, в данном примере сдвиг составил 1.

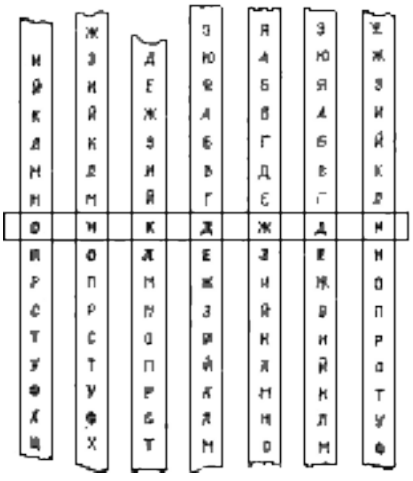


Рис. 2 Метод полосок

Схема шифрования Вижинера

Таблица Вижинера представляет собой квадратную матрицу с n^2 элементами, где n — число символов используемого алфавита. На рисунке 3 показана таблица Вижинера для кириллицы. Каждая строка получена циклическим сдвигом алфавита на символ. Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования.

Осуществляется это следующим образом. Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размещается первая строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе. Пример такой рабочей матрицы для ключа САЛЬЕРИ приведен на рис. 4.

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я
б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а
в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б
г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в
д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д
ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е
з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з
й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
х	ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ь	ъ	ы	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ъ	ы	э	ю	я	а	б	в	г	д	е	з	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
ы	э	ю	я	а	б	в	г	д	е	ж	ж	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ
э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы
ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э
я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ъ	ы	э	ю

Рис. 3 Таблица Вижинера для русского алфавита

Процесс шифрования осуществляется следующим образом:

1. под каждый буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое количество раз;
2. каждая буква шифруемого текста заменяется по подматрице буквами, находящимся на пересечений линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящихся под ними букв ключа;
3. полученный текст может разбиваться на буквы по несколько знаков.

Пусть, например требуется зашифровать сообщение: МАКСИМАЛЬНО ДОПУСТИМОЙ ЦЕНОЙ ЯВЛЯЕТСЯ ПЯТЬСОТ РУБ. ЗА ШТУКУ. В соответствии с первым правилом записываем под буквами шифруемого текста буквы ключа. Получаем:

м а к с и м а л ь н о д о п у с т и м о й ц е н о й я в л я е т с я п я т ь с о т р у б . з а ш т у к у

с а л ь е р и с а л ь е р и с а л ь е р и с а л ь е р и с а л ь е р и с а л ь е р и с а л ь е р и с а

Дальше осуществляется непосредственное шифрование в соответствии со вторым правилом, а именно: берем первую букву шифруемого текста (М) и соответствующую ей букву ключа (С); по букве шифруемого текста (М) входим в рабочую матрицу шифрования и выбираем под ней букву, расположенную в строке, соответствующей букве ключа (С), — в нашем примере такой буквой является Э; выбранную таким образом букву помещаем в шифрованный текст. Эта процедура циклически повторяется до зашифровывания всего текста.

На рис 4 представлена схема шифрования. Эксперименты показали, что при использовании такого метода статические характеристики исходного текста практически не повторяются в зашифрованном сообщении.

Расшифровка текста производится в следующей последовательности:

1. над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое число раз;
2. в строке подматрицы Вижинера, соответствующей букве ключа, отыскивается буква, соответствующая знаку зашифрованного текста. Находящаяся под ней буква первой строки подматрицы и будет буквой исходного текста;
3. полученный текст группируется в слова по смыслу.

На рис. 5 данная процедура представлена в наглядном виде.

Одним из недостатков шифрования по таблице Вижинера является то, что при небольшой длине ключа надежность шифрования остается не высокой, а формирование длинных ключей сопряжено с трудностями.

Нецелесообразно выбирать ключ с повторяющимися буквами, так как при этом стойкость шифра не возрастает. В то же время ключ должен легко запоминаться, чтобы его можно было не записывать. Последовательность же букв, не имеющую смысла, запомнить трудно.

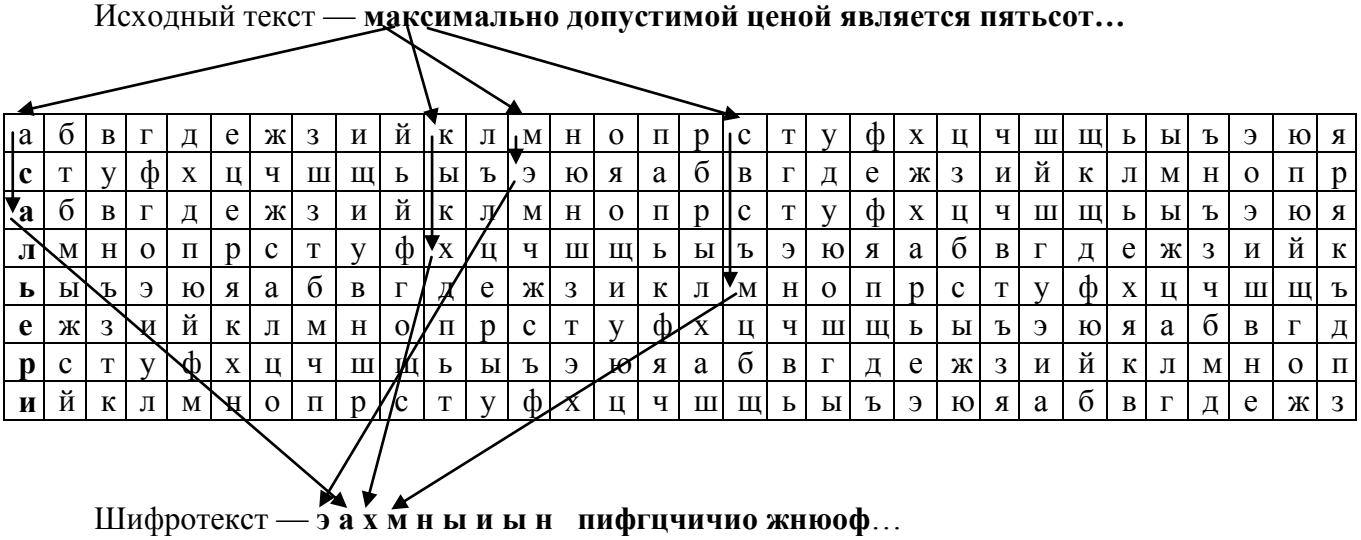


Рис. 4 Последовательность шифрования по таблице Вижинера с использованием ключа «Сальери»

Исходный текст — **м а к с и м а л ь н о**…

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з

Ключ: **с а л ь е р и с а л ь е р и с а л ь е р и с а л ь е р и**

Шифротекст — **эахмныиын пифгцчичио жнюоф**

Рис. 5 Порядок расшифровки по таблице Вижинера

Задание для самостоятельной работы

1. Зашифруйте свою фамилию с помощью **шифра Цезаря**.
2. Дешифруйте сообщение, зашифрованное **шифром Цезаря** (табл. 1) по указанному преподавателем варианту.

Таблица 1

Вар	Шифрограмма (шифр Цезаря)
1	ТСДЗЖЛХЗОЯОБДЛХТУЗЦЕЗОЛЪЛЕГХЯФЛОЦТСДЗЙЖЗРРСЁС
2	ЪЗПШЦЙЗРСЕСФХЯХЗПДСОЯЫЗЛРЧСУПГЩЛЛСРГФСЖЗУЙЛХ
3	ТУГЕЛОГЖОВЕФЗШСЖЛРГНСЕЮЗХСОЯНСЛФНОБЪЗРЛВУГКРЮЗ
4	ЛКСДУЗХГХЗОВНСОЗФГСФСДЗРРСЪХВХДЗОНЛ
5	ДЗФТУЛРЩЛТРСФХЯАХСРЗСХФХЦХФХЕЛЗТУЛРЩЛТСЕГЛШЛКСДЛОЛЗ
6	НГНПГОССНУЮОЗРРЮШФУЗЖЛСНСОЯЩСЕГРРЮШ
7	НХСЕФЗЁЖГФЛЖЛХРГПЗОЛХСХРЛНСЁЖГРЗЦХСРЗХ
8	ХСХЙЛЕЗХТУЛТЗЕГБЪЛНХСЙЛЕЗХТСЖТЗЕГБЪЛ
9	ТУЗЙЖЗЪЗПЕЮШСЖЛХЯЛКФЗДВСТУЗЖЗОЛХЗЖГОЯРЗМЫЛМПГУЫУЦХ
10	СУОЮФЛЖВХОЛДСРГЕЗУЫЛРЗОЛДСЕНОЗХНЗ
11	НСЕГОЯНСРВНЦЗГЙГДГФЕСБРСЁЦФЦЗ
12	РГЦНЛДЮЕГБХЗФХЗФХЕЗРРЮПЛЛТУСХЛЕСЗФХЗФХЕЗРРЮПЛ
13	ВЛФГПЫЦХЛХЯРЗОБДОБЛОБЖВПРЗЖГП
14	ЗФОЛДГУЛРДЗКФГТСЁКРГЪЛХДГУЛРТЗЖГЁСЁ
15	ЛПЗБЬЛМЦЫЛЖГРЗСФХГРЗХФВДЗКОГТЫЛ
16	КГУВЙЗРРСПЦХГРНЦЕЖЦОСРЗФПСХУВХ

3. Зашифруйте свою фамилию с помощью **таблицы Вижинера**. В качестве ключа используйте свое имя.
4. Дешифруйте сообщения, зашифрованные с помощью **таблицы Вижинера** (табл. 2) по указанному преподавателем варианту.

Таблица 2

№ в	Ключ	Шифрограмма (Таблица Виженера)
1	ОБИЛЬНО	ХНШЕТЁЯМКЁЭЛТЯЕГГЭЁБЪБНИЖСНЫУЗЫЭЩБХЪСШГОБЮСЖГГТУЪЭЫЕГМВВЪЦКШПЫУАРЁЦОЁГАЛЯФУТЖАЛАЁТЭАЮ
2	ТУПИК	АОЯЗМТЮГЩИЭЫЬЬЭЫЗГКЕЪЧЭШДЩХЩШЪЯЮЩГЮМЫЧЁШЮМШКВБХВЙЁНВДЩДЭЭХВЮСАИКЧИЪДЮЩНКГЕХЭЭЛЮДШ
3	НИТКА	ЭЗЬЩИАЬЩУББЩЙИНТИПЮЗУТААЕЕЬЭБИЕИМИКТЮСДГБЩРЁУЦАЩИЧКЬЪРПГЁЭСЕЯЬУЩОАААААИАЁПЁАХКПДБЫЫБГЕЦЧСЮМ
4	ДРУЗЬЯ	ЙШОЪИССЭСЫПААОЪБЁРБАСЬХЙГГЮЬФФДЛЛЕМСЬЧПБПЭАОЛЕМЙЙПЬДИГЬВИЁДНУЛЛЩИСБВОЩТСШРСЕИСДПООИЬНЭСЫТЕЫОЩБ
5	ЖИЗНЬ	ЖЧРВЧЛУБЪСВЁКЭЧЭЧЪАМДКЬТЦЩВЖЧОЙЧКЭТКЗЖЙСЗЬЙБЕФЙБЧЫЛЁЯЫЛЖАЖДЦЩЬКДГЕАРОЫЮЗКТРЮЮЬТЦЩДБВФВШУЕМШКЩНЦВЦ
6	ФРЕГАТ	ФЧЖВТЫЛУАДДНШШЬЛГНЮКРКАПЭВЛВЧБНФННУЦНЮЖКЕЪЖСЦМЛИНПАЙННАААААЛЕЫБОЭЧКЭЭЕЪЩПЬНЕПЩФ
7	ЗВЕЗДЫ	КЮЖШЙЧЛЛДГУЙЕСТБЙАБНЙЙОЙЫМДЁОЙИГМЛБЧЙМЖФЕЦЛРЧШОЙГРЙЁБЪЪЮНШБЧЙЛАЩЬМЪГГЬНЧШОЫЦОЦЧЛЫЪБЭШРЧБСТШБЛЛАБ
8	СТРУНА	РЯФНСВЭПЭАЕРККЯЫЗИАЬЫИФПЧАПОЫЧВПБЯФУНЯЪОБЗКЯВСАЫЮЬМЯАЕРЮПДБНБЬЫИЭОПЬЫИДТЯБЭМЫНУЮСХВРВАПЪЕЕЬЫК
9	СВЕЧА	ААЙЙОТЮШЫОЮОЫКОРЩЬСРОРЧЪДВЦЙЖЛЧЦЧЪОРГНЬЯАЪЙШЛОРААТЭЛЫХЛМЯДЫЬЦЮТЫОЬЮЗЬМЧОЫЫЬЬЮТЫОААЙЖСРГТЬНУЧЫМНЭРЛИТЧРЧ
10	ПОМПЕЯ	ЮЪЕЫЙММЬВАЛПЗЪИЮАДЬЕГХАГВЦЁХЁУЯУФДЯОЩИБЯЗВХЩЖЭДЙАВШЫЛБВЯВАЙНЮРВАЙНАЦШЯКАГНЕХЖЙЬЪЕМИБТЦЫДЭЙЩ
11	СВОБОДА	ЮОЪЬМУНЙГТДЩИОЪАГСУПЮБЛСПААЫПГЩЖУПЧЫЩЦВАМЛОЛРСББТВУЪЛМНОЦВСММАЛНПИЯГОЬНЖГБАЭОТЩЬЯЬМЫПЮХКРЛОЪГДЯЪПХЧ
12	ОДИНОЧКА	ЬКЪЦСЦЮБЕАУФБЧЖЛЦАИЕУСЮПАОЁЯЯЧЩАШБЩУЕУЧАВЕЖБЮНЖТРОИЕВЧМКЕУЙБГМЪЛСЙЕБЦЪАОБКДЫФЬЁТАИЗТГЮБЕТЧЩТЦЫААШАТЬУЧЩИЯКОЭЕ
13	ЗАПРЕТ	ПТЯРЭИЯИГЛДЭИОЧШНЙЁАНВЙЪЙВХВАЭЖКРЧАЪДЯЮФМПБХЮГННЙОВШЯТИЖЩБАОЧНРВЛЬВСГСАЫЁОЭЧЫЭИЕГФИТЩОЪБЪЫЭНРУАЧЙЯЮФКЮЖСЩ
14	КАРТЫ	КОВМНЖЛПСУЖТФЫЕЭАААФДСАНМИДСБСЮДВЦИДРЮРЕВНФЩБЭЯЮСТДЙЪЬРДДЮЧПХРВЦЗЁАВЙНЖДЛМЖДЛЮЪНЖБЮРУВ
15	РАЗЛУКА	ФСДЭЭЧЕВСЧЧШИБЮКШУЮЧЯЧЬЩГШСРПЗИПОХВААПЗСЗСОСЖАИУХЮРЖМЫЁАБСКФОХТЛСЧЁЩЪЯБЬЁФРЖОРОВВМЩРПЗДЗЧДЙЭАЬХЫБЬН
16	НАУКА	СОВБАЦЕШАНТУДГЫЯКЪЮЖЭАЩГЕВОЯДМЁЧЯДБНЛШЪНЫВАМЕАЬЛАОГЕЪСГБРСАСЮИЕАОЯАЬБОЦКМАПГАОЮЛБЧСЁВЫВ

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Партыка Т. Л., Попов И. И. Информационная безопасность: учебное пособие/ Т. Л. Партыка, И. И. Попов. — 3-е изд., перераб. и доп. — М.: ФОРУМ, 2010. — 432 с.:ил. — (Профессиональное образование)
2. Файловый архив студентов StudFiles [Электронный документ] — URL: http://www.studfiles.ru