Информационная безопасность

- **Первый способ** – это чисто *силовые методы охраны* документа (носителя информации) физическими лицами, его передача специальным курьером и т.д.
- **Второй способ** получил название *«стеганография»* и заключался в сокрытии самого факта наличия секретной информации. В этом случае, в частности, использовались так называемые «симпатические чернила». При соответствующем проявлении текст становился видимым.
- **Третий способ** информации заключался в преобразовании смыслового текста в некий хаотический набор знаков (букв алфавита). Получатель донесения имел возможность преобразовать его в исходное осмысленное сообщение, если обладал «ключом» к его построению. Этот способ защиты информации называется *криптографическим.*

ГОСТ "Защита информации. Основные термины и определения" вводит понятие **информационной безопасности** как состояние ***защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность***.

- **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Под *угрозой безопасности информации* понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов системы, а также программных и аппаратных средств

Угрозы информационной (компьютерной) безопасности

Угрозы информационной (компьютерной) безопасности – это различные действия, которые могут привести к нарушениям информационной безопасности. Другими словами, это потенциально возможные события/процессы или действия, которые могут нанести ущерб информационным и компьютерным системам.

Информационные угрозы

Случайные:

Ошибки пользователя

Ошибки в програмировании

Отказ, сбой аппаратуры

Форс-мажорные обстоятельства

Преднамеренные:

Хищение информации

Компьютерные вирусы

Физическое воздействие на аппаратуру

Виды умышленных угроз безопасности информации:

- ***Пассивные угрозы*** направлены в основном на несанкционированное использование информационных ресурсов ИС, не оказывая при этом влияния на ее функционирование. Например, несанкционированное использование базы данных, прослушивание каналов связи и т.п.
- ***Активные угрозы*** имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компьютер. Источником активных угроз могут быть действия взломщиков, вредоносные программы и т.п.

Информационные угрозы:

нарушение доступности

уничтожение информации

отрицание подлинности представляемой информации

хищение или копирование

искажение информации (искажение, нарушение целостности)

введение ложной информации

К основным угрозам безопасности информации и нормального функционирования ИС относятся:

- ***Утечка конфиденциальной информации*** - бесконтрольный выход конфиденциальной информации за пределы ИС;
- ***Компрометация информации*** - несанкционированные изменения в базе данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений;
- ***Несанкционированное использование информационных ресурсов*** является следствием ее утечки и средством ее компрометации;
- ***Ошибочное использование информационных ресурсов*** может привести к разрушению, утечке или компрометации указанных ресурсов;
- ***Несанкционированный обмен информацией*** *между* абонентами может привести к получению одним из них сведений, доступ к которым ему запрещен;
- ***Отказ от информации*****;** состоит в непризнании получателем или отправителем этой информации фактов ее получения или отправки. Это позволяет одной из сторон расторгать заключенные финансовые соглашения «техническим» путем, формально не отказываясь от них, нанося тем самым второй стороне значительный ущерб.
- ***Нарушение информационного обслуживании*** - задержка с предоставлением информационных ресурсов абоненту, которая может привести к тяжелым последствиям.
- ***Незаконное использование привилегий*** - большинство систем защиты используют наборы привилегий. Обычно пользователи имеют минимальный набор привилегий, администраторы — максимальный. Наборы привилегий охраняются системой защиты.
- ***Незаконный захват привилегий*** возможен при наличии ошибок в системе защиты, но чаще всего происходит при небрежном пользовании привилегий.

Вирус — **программа, которая может заражать другие программы путем включения в них модифицированной копии, обладающей способностью к дальнейшему размножению**.

Вирус характеризуется двумя основными особенностями:

- способностью к саморазмножению;
- способностью к вмешательству в вычислительный процесс

Классификация вирусов

Логические бомбы

Логическая бомба (англ. *Logic bomb*) —программа, которая запускается при определенных временных или информационных условиях для осуществления вредоносных действий, чаще для искажения или уничтожения данных, реже с их помощью совершаются кража или мошенничество.

Реальный пример логической бомбы: программист, предвидя свое увольнение, вносит в программу расчета заработной платы определенные изменения, которые начинают действовать, когда его фамилия исчезнет из набора данных о персонале фирмы,

Троя́нская программа **(также —** троян, троянец, троянский конь, трой**)**

" Троянский конь" - это программа, которая, маскируясь под полезную программу, выполняет дополнительные функции, о чем пользователь и не догадывается (например, собирает информацию об именах и паролях, записывая их в специальный файл, доступный лишь создателю данного вируса, либо разрушает файловую систему).

Для того, чтобы спровоцировать пользователя запустить троянца, файл программы называют служебным именем, маскируют под другую программу (например, установки другой программы), файл другого типа или просто дают привлекательное для запуска название, иконку и т. п. Злоумышленник может перекомпилировать существующую программу, добавив к её исходному коду вредоносный, а потом выдавать за оригинал или подменять его.

Репликаторные программы

Благодаря своему быстрому воспроизводству приводят к переполнению основной памяти. Уничтожение программ-репликаторов усложняется, если воспроизводимые программы не являются точными копиями оригинала.

Мутанты

Изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.

Самовоспроизводятся, причем вновь созданные копии значительно отличаются от оригинала.

Поскольку этот вирус постоянно изменяется, его очень сложно обнаружить с помощью стандартных средств.

Вирусы-невидимки (стелс-вирусы)

Вирус, полностью или частично скрывающий свое присутствие в системе.

Эти вирусы перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо них незараженные объекты.

Иногда такие вирусы при запуске любой программы (включая антивирус) восстанавливают зараженные сектора, а после окончания ее работы снова заражают диск.

К числу наиболее характерных признаков заражения компьютера вирусами относятся следующие:

- некоторые ранее исполнявшиеся программы перестают запускаться или внезапно останавливаются в процессе работы;
- увеличивается длина исполняемых файлов;
- быстро сокращается объём свободной дисковой памяти;
- на носителях появляются дополнительные сбойные кластеры, в которых вирусы прячут свои фрагменты или части повреждённых файлов;
- замедляется работа некоторых программ;
- в текстовых файлах появляются бессмысленные фрагменты;
- на экране появляются странные сообщения, которые раньше не наблюдались;
- появляются файлы со странными датами и временем создания (несуществующие дни несуществующих месяцев, годы из следующего столетия, часы, минуты и секунды, не укладывающиеся в общепринятые интервалы и т. д.);
- операционная система перестаёт загружаться с винчестера;
- появляются сообщения об отсутствии винчестера;
- данные на носителях портятся.

Требования к антивирусным программам:

- ***Стабильность и надежность работы*.**
- ***Размеры вирусной базы программы*** (количество вирусов, которые правильно определяются программой).
- ***Скорость работы программы, наличие дополнительных возможностей***
- ***Многоплатформенность***

Все антивирусные программы можно разделить на следующие группы:

- детекторы
- ревизоры;
- фильтры;
- доктора (фаги);
- вакцины

. *Программы-детекторы* обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные

- **Универсальные детекторы** в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов.
- **Специализированные детекторы** выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы.
- Детектор, позволяющий обнаруживать несколько вирусов, называют **полидетектором**.
- Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-ревизоры.

- Надежным средством защиты от вирусов считаются **программы-ревизоры.** Они запоминают исходное состояние программ, каталогов и системных областей диска, когда компьютер еще не был заражен вирусом, а затем периодически сравнивают текущее состояние с исходным. При выявлении несоответствий (по длине файла, дате модификации, коду циклического контроля файла и др.) сообщение об этом выдается пользователю.
- Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом.

Программы-фильтры, или «сторожа», **выявляют действия, характерные для вирусов, при обнаружении таких действий посылают запрос пользователю для подтверждения правомерности таких процедур.**

- Программы-фильтры, постоянно находятся в оперативной памяти, и «перехватывают» все запросы к операционной системе на выполнение «подозрительных действий», т.е. операций, используемых вирусами для своего размножения и порчи информационных и других системных ресурсов в компьютере. Такими действиями могут быть. попытки изменения атрибутов файлов, коррекции исполняемых файлов, записи в загрузочные сектора диска и др. При каждом запросе на такое действие на экран компьютера выдается сообщение об этих действиях и о том, какая программа желает их выполнять. Пользователь в ответ на это должен либо разрешить выполнение действия, либо запретить его.
- Подобная часто повторяющаяся «назойливость», раздражающая пользователя, и то, что объем оперативной памяти уменьшается из-за необходимости постоянного нахождения в ней «сторожа», являются главными недостатками этих программ. К тому же программы-фильтры не «лечат» файлы или диски, для этого необходимо использовать другие антивирусные программы.

Доктора

– самый распространенный и эффективный вид антивирусных программ. К ним относятся Антивирус Касперского, Doctor Wed, Norton Antivirus, которые не только находят вирусы, но и лечат зараженные вирусами файлы и секторы дисков, «выкусывая» из зараженных программ тело вируса. Они сначала ищут вирусы в оперативной памяти и уничтожают их там, затем лечат файлы и диски.

Программы этого типа делятся на фаги и полифаги. Последние служат для обнаружения и уничтожения большого количества разнообразных вирусов. Наибольшее распространение в России имеют такие полифаги, как MS AntiVirus, Aidstest и Doctor Web, которые непрерывно обновляются для борьбы с появляющимися новыми вирусами.

Программы-вакцины, или иммунизаторы

относятся к резидентным программам.

Они модифицируют файлы или диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает их уже зараженными и не внедряется в них.

HOME USER WINDOWS

22 Internet security suites
put to the test under Windows 10

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Manufacturer	Product	AV-TEST Certificate	Protection (max. 6 pts)	Performance (max. 6 pts)	Usability (max. 6 pts)	Overall Points Total (max. 18)
AhnLab	V3 Internet Security	TOP PRODUCT	6.0	6.0	6.0	18.0
Avira	Antivirus Pro	TOP PRODUCT	6.0	6.0	6.0	18.0
F-Secure	SAFE	TOP PRODUCT	6.0	6.0	6.0	18.0
G Data	Internet Security	TOP PRODUCT	6.0	6.0	6.0	18.0
Kaspersky	Internet Security	TOP PRODUCT	6.0	6.0	6.0	18.0
McAfee	Total Protection	TOP PRODUCT	6.0	6.0	6.0	18.0
Microsoft	Defender Antivirus	TOP PRODUCT	6.0	6.0	6.0	18.0
NortonLifeLock	Norton 360	TOP PRODUCT	6.0	6.0	6.0	18.0
Avast	Free Antivirus	TOP PRODUCT	6.0	5.5	6.0	17.5
AVG	Internet Security	TOP PRODUCT	6.0	5.5	6.0	17.5
Bitdefender	Internet Security	TOP PRODUCT	6.0	6.0	5.5	17.5
BullGuard	Internet Security	TOP PRODUCT	6.0	6.0	5.5	17.5
ESET	Internet Security	TOP PRODUCT	6.0	5.5	6.0	17.5
Protected.net	Total AV	TOP PRODUCT	5.5	6.0	6.0	17.5
Trend Micro	Internet Security	TOP PRODUCT	6.0	5.5	6.0	17.5
VIPRE Security	AdvancedSecurity	TOP PRODUCT	5.5	6.0	6.0	17.5
K7 Computing	TotalSecurity		4.5	6.0	6.0	16.5
Microworld	eScan Internet Security Suite		4.0	6.0	5.5	15.5
Heimdal Security	Thor Premium		3.0	6.0	5.5	14.5
Malwarebytes	Premium		5.5	4.5	4.5	14.5
PC Matic	PC Matic		3.0	6.0	4.5	13.5
Cylance	Smart Antivirus		2.5	6.0	3.5	12.0

Антивирусы	Защита	Производительность	Юзабилити	Общее
AhnLab V3 Internet Security	6.0/6	6.0/6	6.0/6	**18.0**
AVIRA Antivirus Pro	6.0/6	6.0/6	6.0/6	**18.0**
F-Secure SAFE	6.0/6	6.0/6	6.0/6	**18.0**
G Data Internet Security	6.0/6	6.0/6	6.0/6	**18.0**
Kaspersky Internet Security	6.0/6	6.0/6	6.0/6	**18.0**
McAfee Total Protection	6.0/6	6.0/6	6.0/6	**18.0**
Microsoft Defender Antivirus	6.0/6	6.0/6	6.0/6	**18.0**
NortonLifeLock Norton 360	6.0/6	6.0/6	6.0/6	**18.0**

Существует ряд правил, выполнение которых позволяет защитить компьютер от вирусов:

- иметь на компьютере пакет антивирусных программ и периодически их обновлять;
- не пользоваться чужими флешками без предварительной проверки их антивирусными программами;
- не запускать программы, назначение которых неизвестно;
- не раскрывать вложения в электронные письма от неизвестных лиц;
- периодически проверять все носители информации на наличие вирусов;
- после разархивирования архивных файлов проверять их на наличие вирусов;
- использовать только лицензионные программные продукты.

Организация систем защиты информации

Система защиты информации – это совокупность мер правового и административного характера, организационных мероприятий, программно-аппаратных средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности.

Известны следующие основные методы защиты информации:

- Создание препятствий
- Управление доступом
- Маскировка
- Регламентация
- Принуждение

Создание препятствий – метод физического преграждения пути к защищаемой информации.

Управление доступом **– метод защиты информации с помощью разделения прав доступа пользователей к ресурсам компьютерной информационной системы.**

Этот метод включает в себя следующие процедуры:

- идентификацию пользователей, т.е. присвоение им уникальных имен и кодов;
- проверку того, что лицо, сообщившее идентификатор, является подлинным лицом (аутентификация пользователей);
- проверка полномочий, т.е. проверка права пользователей на доступ к системе или запрашиваемым данным;
- автоматическая регистрация в специальном журнале всех запросов к информационным ресурсам.

Маскировка - метод защиты информации путем её криптографического* закрытия.

Этот метод защиты заключается в преобразовании (шифровании) основных частей информации (слов, букв, цифр, слогов) с помощью специальных алгоритмов, в результате чего нельзя определить содержание данных не зная ключа.

На практике используются два типа шифрования: симметричное и ассимметричное. При симметричном шифровании для шифрования и дешифрования используется один и тот же ключ. Ассимметричное шифрование основано на том, что для шифрования и дешифрования используются разные ключи, связанные друг с другом. Знание одного ключа не позволяет определить другой. Один ключ свободно распространяется и является открытым (public key), второй ключ известен только его владельцу и является закрытым (private key).

* Криптография – это наука об обеспечении секретности и подлинности сообщений. (крипто –тайна, графия – письмо)

Регламентация

– метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которой возможности несанкционированного доступа к ней становятся минимальными.

Принуждение

метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования информации под угрозой материальной, административной или уголовной ответственности

Шифруемая буква

Буква ключа

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
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 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 Ы Ъ 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 Ы Ъ Э Ю Я А Б В
……
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
……
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 Л
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 Л М
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 Л М Н
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 Л М Н О
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
……
Я А Б В Г Л Е Ж З И Й К Л М Н О П Р СТ У Ф Х Ц Ч Ш Щ Ь Ы ЪЭ ЮЯ

Таблица Вижинера

Устанавливается ключ – некоторое слово или набор букв, например МОРЕ. Шифровать будем слово ЗАЩИТА

Процесс шифрования состоит в следующем:

1.Под каждой буквой шифруемого текста записываются буквы ключа, повторяющие ключ требуемое число раз.

ЗАЩИТА

МОРЕМО

2. Буква шифруемого текста определяет столбец таблицы, а буква ключа – её строку. Зашифрованная буква находится на пересечении столбца и строки.

Полученное слово: УОЙНЭО

Расшифровка предполагает выполнение обратной процедуры:

1. над буквами зашифрованного текста сверху последовательно записываются буквы ключа;
2. буква ключа определяет строку таблицы, а буква зашифрованного текста – его столбец. Буква, находящаяся в первой строке таблицы, является буквой расшифрованного текста.

Обеспечение информационной безопасности в любой компании предполагает следующее.

1. Определение целей обеспечения информационной безопасности компьютерных систем.
2. Создание эффективной системы управления информационной безопасностью.
3. Расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям.
4. Применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния.
5. Использование методик управления безопасностью с обоснованной системой метрик и мер обеспечения информационной безопасности, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

И помните, безопасность информации зависит только от Вас

Международные и отечественные стандарты информационной безопасности и их методическое обеспечение

В настоящее время в России наряду с отечественной нормативной базой широко используются около 140 международных стандартов в области информационных технологий. Из них около 30 затрагивают вопросы защиты информации. Некоторые международные стандарты по защите информации приняты и введены в действие в России, но эти стандарты не составляют целостной основы для решения проблем информационной безопасности, особенно в части нормативного регулирования, методического и инструментального обеспечения разработки, оценки и сертификации безопасности ИТ с учетом современного уровня развития, масштабов и многообразия угроз.

В последнее время в разных странах появилось новое поколение стандартов в области защиты информации, посвященных практическим вопросам управления информационной безопасности компании.

Это, прежде всего, международные и национальные стандарты управления информационной безопасностью ISO 15408, ISO 17799 (BS 7799), BSI; стандарты аудита информационных систем и информационной безопасности COBIT, SAC, COSO и некоторые другие, аналогичные им

Результатом проведения аудита в последнее время все чаще становится сертификат, удостоверяющих соответствие обследуемой ИС требованиям признанного международного стандарта.

Сертификация на соответствие стандарту позволяет наглядно показать деловым партнерам, инвесторам и клиентам, что в компании налажено эффективное управление информационной безопасностью.

Это обеспечивает компании конкурентное преимущество, демонстрируя способность управлять информационными рисками.

Процесс сертификации на соответствие требованиям стандарта предполагает несколько этапов:

- ***Предварительная оценка системы управления ИБ и диагностика.***
- ***Сертификационный аудит.***
- ***Поддержка действия сертификата.***