Зки

1. Информационная безопасность является составной частью концепции национальной безопасности РБ. Под ИБ понимается состояние защищенности интересов личности, общества, гос-тва от внутренних и внешних угроз.

Основные задачи:

1. Право граждан на тайну телефонных и иных сообщений и тд.
2. Защита сведений относящейся к коммерческой, служебной тайнам.
3. Обеспечение инф.систем и сетей связи и много другое

Актуальность проблем защиты информации в компьютерных ИС обусловлено следующими причинами:

1. Увеличение мощности ПК и упрощение их эксплуатации.
2. Увеличение обьемов информации хранимой на ПК
3. Темпы роста кол-ва ПК
4. Резкое расширение круга пользователей имеющих доступ к выч.ресурсам
5. Рост программного обеспечения
6. Повсеместное распространение сетевых технологий
7. Проблемы защиты информации хранящиеся в цифровой форме напрямую связано с эл. Сигналами электро-магнитными полями, которые предоставлены возможность передачи сообщений, однако развитие выч. Техники расширило диапазон угроз.

Угрозы безопасности – это потенциально возможное событие, действие, процесс, которое может привести к нанесению материального, морального и иного ущерба защищенному объекту.

Классификация угроз:

1. По природе возникновения
2. Естественные
3. Искусственные
4. По целям злоумышленника
5. Угрозы конфиденциальности данных
6. Угрозы целостности
7. Угрозы доступности
8. Угрозы отказа от выполнения транзакции
9. По обьекту защите
10. Внешние
11. Внутренние
12. Проблемы защиты информации хранящиеся в цифровой форме напрямую связано с эл. Сигналами электро-магнитными полями, которые предоставлены возможность передачи сообщений, однако развитие выч. Техники расширило диапазон угроз.

Угрозы безопасности – это потенциально возможное событие, действие, процесс, которое может привести к нанесению материального, морального и иного ущерба защищенному объекту.

Методы защиты:

* Препятствие управление доступом – включает в себя: идентификацию пользователей и ресурсов посредством персональных идентификаторов, а так же аутентификацию.
* Маскировка – представляет собой преобразование информации, в следствии чего она становится недоступной и непонятной для нарушителя.
* Регламентация – заключается в разработке и реализации комплекса мероприятий по обработке и воздействия угроз
* Принуждение – метод, при котором пользователей вынуждают соблюдать правила работы с информацией под угрозой(моральной, уголовной, материальной)
* Побуждение – тонкая грань с принуждением. Метод защиты, при котором материальные, моральные, этические нормы побуждают к соблюдению правил работы с инф.

1. Проблемы защиты информации хранящиеся в цифровой форме напрямую связано с эл. Сигналами электро-магнитными полями, которые предоставлены возможность передачи сообщений, однако развитие выч. Техники расширило диапазон угроз.

Угрозы безопасности – это потенциально возможное событие, действие, процесс, которое может привести к нанесению материального, морального и иного ущерба защищенному объекту.

Средства защиты(бывают формальные/неформальные) рассматриваются как последовательность рубежей информации.

Выделяют 4 рубежа:

1. Соблюдение юрид.норм
2. Морально-этические средства
3. Организационные средства защиты
4. Технические средства защиты
5. Проблемы защиты информации хранящиеся в цифровой форме напрямую связано с эл. Сигналами электро-магнитными полями, которые предоставлены возможность передачи сообщений, однако развитие выч. Техники расширило диапазон угроз.

Угрозы безопасности – это потенциально возможное событие, действие, процесс, которое может привести к нанесению материального, морального и иного ущерба защищенному объекту.

Законодательная база в области безопасности:

В РБ эту базу составляют:

1. Концепция нац. Безопастности РБ
2. Законы об информации, защите информации; о гос секретах; гражданский/уголовный кодекс; постановление совета министра;руководящий документ нац банка.
3. Идентификация – процесс распознавания элемента системы, с помощью заранее определенного идентификатора.

Аутентификация – это проверка подлинности идентификации пользователя, процесса, устройства.

Требования:

1. Должен требовать от пользователей идентифицировать себя при запросах на доступ
2. Подверкать проверке подлинность идентификации(аутентифицировать)
3. Комплекс должен располагать необходимыми данными для идентификации и аутент.
4. Препятствовать доступу к защищаемым ресурсам.

Биометрическая идентификация – это предьявление пользователям своего уникального биометрического параметра и процесс сравнивания его с базой имеющихся.

Статические методы Б.И:

1. Отпечаток п.
2. Днк
3. Окустич. Часть уха
4. Рисунок вен
5. Геометрия руки
6. Термограмма тела

Динамические методы Б.И:

1. Голос
2. Рукописный подчерк
3. Клавиатурный подчерк.
4. Вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Червь – программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее. Отличительной особенностью червя является то, что он не может стать частью другой безвредной программы.

Троянская программа (троянский конь, троян)

Троянская программа маскируется в других безвредных программах. До того момента как пользователь не запустит эту самую безвредную программу, троян не несет никакой опасности. Тронская программа может нанести различный ущерб для компьютера. В основном трояны используются для кражи, изменения или удаления данных. Отличительной особенностью трояна является то, что он не может самостоятельно размножаться.

Программы – шпионы

Шпионы собирают информацию о действиях и поведении пользователя. В основном их интересует информация (адреса, пароли).

Зомби

Зомби позволяют злоумышленнику управлять компьютером пользователя. Компьютеры – зомби могут быть объединены в сеть и использоваться для массовой атаки на сайты или рассылки спама. Пользователь может не догадываться, что его компьютер зомбирован и используется злоумышленником

Программы – блокировщики (баннеры)

Это программа, которая блокирует пользователю доступ к операционной системе. При загрузке компьютера появляется окно, в котором пользователя обвиняют в скачивание нелицензионного контента или нарушение авторских прав. И под угрозой полного удаления всех данных с компьютера требуют отослать смс на номер телефона или просто пополнить его счет. Естественно после того как пользователь выполнит эти требования банер никуда не исчезнет.

Вредоносная программа (Malware) – это любое программное обеспечение, созданное для получения несанкционированного доступа к компьютеру и его данным, с целью хищения информации или нанесению вреда. Термин “Вредоносная программа” можно считать общим для всех типов компьютерных вирусов, червей, троянских программ и тд.

Виды антивирусов:

1. Программы-детекторы, или сканеры, находят вирусы в оперативной памяти и на внешних носителях, выводя сообщение при обнаружении вируса.
2. Программы-доктора, (фаги, программы-вакцины) находят зараженные файлы и "лечат" их. Среди этого вида программ существуют полифаги, которые способны удалять разнообразные виды вирусов, самые известные из антивирусов-полифагов Norton AntiVirus, Doctor Web, Kaspersky Antivirus.
3. Программы-ревизоры являются наиболее надежными в плане защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера, затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей.
4. Программы-мониторы (файерволы, брандмауэры) начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу "здесь и сейчас".
5. Программы-фильтры (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться. Программы-сторожа - небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.

**8** Криптография – это наука о защите информации с использованием математических основ

Обратная криптографии наука, занимающаяся методомвскрытия информации называется криптоанализ.

Проблема использования криптографических методов актуальна, так как расширилась возможность использования компьютерных сетей. Появляется развитие нейронных сетей, вычислений и тд.

Шифрование данных – это один из важнейших элементов системы инф. Безопасности, использующий грамотную настройку системы разграничения доступа.

Шифр замен является простейшим, наиболее популярным шифром. Типичными примерами являются шифр Цезаря, ``цифирная азбука'' Петра Великого и ``пляшущие человечки'' А.Конан Дойла. Как видно из самого названия, шифр замены осуществляет преобразование замены букв или других ``частей'' открытого текста на аналогичные ``части'' шифрованного текста. Легко дать математическое описание шифра замены. Пусть и- два алфавита (открытого и шифрованного текстов соответственно), состоящие из одинакового числа символов. Пусть также- взаимно-однозначное отображение. Тогда шифр замены действует так: открытый текст преобразуется в шифрованный текст.

Шифр перестановки, как видно из названия, осуществляет преобразование перестановки букв в открытом тексте. Типичным примером шифра перестановки является шифр ``Сцитала''. Обычно открытый текст разбивается на отрезки равной длины и каждый отрезок шифруется независимо. Пусть, например, длина отрезков равнаи- взаимнооднозначное отображение множествав себя. Тогда шифр перестановки действует так: отрезок открытого текстапреобразуется в отрезок шифрованного текста. Шифр заменыявляется простейшим, наиболее популярным шифром. Типичными примерами являются шифр Цезаря, ``цифирная азбука'' Петра Великого и ``пляшущие человечки'' А.Конан Дойла. Как видно из самого названия, шифр замены осуществляет преобразование замены букв или других ``частей'' открытого текста на аналогичные ``части'' шифрованного текста. Легко дать математическое описание шифра замены. Пустьhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-AKCesO.pngиhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-uWY_47.png- два алфавита (открытого и шифрованного текстов соответственно), состоящие из одинакового числа символов. Пусть такжеhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-RjIJ5L.png- взаимнооднозначное отображениеhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-U73PwJ.pngвhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-HTrkLr.png. Тогда шифр замены действует так: открытый текстhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-TRd4IQ.pngпреобразуется в шифрованный текстhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-r7uvuE.png.

Шифр перестановки, как видно из названия, осуществляет преобразование перестановки букв в открытом тексте. Типичным примером шифра перестановки является шифр ``Сцитала''. Обычно открытый текст разбивается на отрезки равной длины и каждый отрезок шифруется независимо. Пусть, например, длина отрезков равнаhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-yeJuvP.pngиhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-5TvvQN.png- взаимнооднозначное отображение множестваhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-I59fhP.pngв себя. Тогда шифр перестановки действует так: отрезок открытого текстаhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-OHQHND.pngпреобразуется в отрезок шифрованного текстаhttps://studfiles.net/html/2706/378/html_xfDC1EEM29.WyY0/img-GKiqpd.png.

**9.** Симметри́чные криптосисте́мы— способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами.

Классическими примерами таких алгоритмов являются симметричные криптографические алгоритмы, перечисленные ниже:

1. Простая перестановка
2. Одиночная перестановка по ключу
3. Двойная перестановка
4. Перестановка "Магический квадрат"

Классификация:

1. Простая перестановка без ключа — один из самых простых методов шифрования. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифртекста он считывается по строкам. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы. Объединение букв в группы не входит в ключ шифра и используется лишь для удобства записи несмыслового текста.
2. Одиночная перестановка по ключу Более практический метод шифрования, называемый одиночной перестановкой по ключу, очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.
3. Двойная перестановка Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов отличались от длин в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным
4. Маги́ческий, или волше́бный квадра́т — квадратная таблица , заполненная различными числами таким образом, что сумма чисел в каждой строке, каждом столбце и на обеих диагоналях одинакова. Если в квадрате равны суммы чисел только в строках и столбцах, то он называется полумагическим.