Нестеренко Пётр Алексеевич. КПБО2-8

Контрольная работа.

Вариант №4

1) Российский стандарт блочного шифрования "Кузнечик": основные параметры, структура раунда (цикла) шифрования и принцип действия, процедура разворачивания исходного ключа в раундовые (рабочие подключи), режимы использования.

Ответ: Алгоритм шифрования „Кузнечик" – блочный алгоритм симметричного шифрования на основе SP-сетей. Параметры: длина ключа 256 бит, размер блока 128 бит, количество раундов шифрования - 10. Шифрование производится на основе 3-х преобразований ~~над блоком данных~~: побитовый XOR блока данных с раундовым ключом (X-функция), побайтовая замена (S-функция), линейное преобразование (умножение в полях Галуа). Генерация раундовых ключей производится с помощью SP-сети 256-битный исходный ключ разбивается пополам, и

левой частью производятся X, S и L функции, пара-
чего происходит еще один дополнительный ход
с итер. const
~~блок~~ с правой частью исходного плана.

(2). Назовите метод выявления вредоносных программ на основе эвристического поиска, приведите его достоинства и недостатки.

Эвристический анализ - метод обнаружения вредоносных программ, при котором антивирусная программа контролирует все действия, выполняемые проверяемой программой. В ходе эвристического анализа отслеживаются потенциально опасные действия, характерные для вирусов вредоносных программ других типов. Достоинства: контролируя действия проверяемых программ, эвристический анализатор современных антивирусов способен обнаружить новые, неизвестные вирусы ещё до того, как эти вирусы начали действовать.

Недостатки: чрезмерная подозрительность эвристического анализатора может вызывать ложные срабатывания при наличии в программе фраг-

...ментов кода, выполняющего действия с ними пользовательности, в том числе и свойственные некоторым вирусам.

5) Понятие защищённой ОС (типичные атаки на ОС. Что такое защищённая операционная система? Политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых ОС.

Защищённая операционная система - это ОС, предусматривающая средства защиты от основных классов угроз безопасности. Защищённая ОС обязательно должна содержать средства разграничения доступа к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с ОС. Кроме того защищённая ОС должна содержать средства противодействия несанкционированному выводу ОС из строя. Политика безопасности - это набор норм, правил и практических приемов, регулирующих порядок хранения и обработки ценной информации. Адекватная политика безопасности - политика безопасности, обеспечивающих ~~порядок хране~~

ная и обработка цепной информации. достаточная уровень защищённости ОС. Адекватность политики безопасности определяется не только архитектурой ОС, но и её конфигурацией, установленными программами и т.д. Существует два основных подхода к созданию защищенных ОС: фрагментарный и комплексный. Фрагментарный подход - это подход, предполагающий организацию защиты вначале от одной угрозы, затем от другой и т.д. Примером фрагментарного подхода является установка на незащищённую ОС антивирусного пакета, системы шифрования и т.д. Комплексный подход - это подход, предполагающий внесение защитных функций в ОС на этапе проектирования её архитектуры. При этом защитные функции являются неотъемлемой частью ОС. Типичные атаки на ОС: сканирование файловой системы, кража ключевой информации, подбор пароля, сборка мусора, превышение полномочий, программные закладки, жадные программы.

4) Шлюз прикладного уровня (назначение, принцип работы, достоинства и недостатки)

Шлюз прикладного уровня, называемый также прикладным шлюзом или экранирующим шлюзом, функционирует на прикладном уровне модели OSI, охватывает также уровень представления и обеспечивает наиболее надёжную защиту межсетевых взаимодействий (идентификация и аутентификация, разграничение доступа, поиск вирусов).

Принцип работы: Прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, исключая тем самым прямые соединения между внутренней и внешней сетью. Если для какого-либо из приложений отсутствует свой посредник, то прикладной шлюз не сможет обрабатывать трафик такого приложения, и он будет заблокирован. Достоинства: высокий уровень защиты локальной сети, нарушение работоспособности прикладного шлюза, не влияет безопасность защищаемой сети (т.к. блокируется сквозное прохождение пакетов

возможность осуществления большого кол-ва дополнительных проверок. Недостатки: очень ощутительно высокая стоимость, довольно большая сложность межсетевого экрана, высокие требования к производительности компьютерной платформы, отсутствие прозрачности для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.