**Нестеренко Пётр Алексеевич КТбо2-8**

**Контрольная работа 19.12.2020**

**Вариант №4**

**Вопросы:**

* ***Вопрос №****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.
* ***Вопрос №2***: Поясните метод выявления вредоносных программ на основе эвристического поиска, приведите его достоинства и недостатки.
* ***Вопрос №3*:** Понятие защищённой операционной системы (Типичные атаки на операционные системы. Что такое защищённая операционная система, политика безопасности и адекватная политика безопасности? Приведите основные подходы к построению защищённых операционных систем.)
* ***Вопрос №4*** Шлюз прикладного уровня (назначение, принцип работы, достоинства и недостатки).

**Ответы:**

1. **Алгоритм шифрования Кузнечик** – это блочный алгоритм симметричного шифрования на основе SP-сетей. Параметры: длина ключа 256 бит, размер блока 128 бит, количество раундов шифрования – 10. Шифрования производится на основе трёх преобразований: побитовый XORблока данных с раундовым ключом (X-функция), побайтовая замена (S-функция), и линейное преобразование (умножение в полях Галуа). Генерация раундовых ключей производится с помощью SP-сети. 256-битный исходный ключ разбивается пополам, над левой частью производятся X,S и L функции, после чего происходит ещё один дополнительный XOR c правой частью исходного ключа.
2. **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 и вредоносных программ других типов. **Достоинства:** Контролируя действия проверяемых программ, эвристический анализатор современных антивирусов способен обнаружить новые, неизвестные вирусы еще до того, как эти вирусы начали действовать. **Недостатки:** резмерная подозрительность эвристического анализатора может вызывать ложные срабатывания при наличии в программе фрагментов кода, выполняющего действия и/или последовательности, в том числе и свойственные некоторым вирусам.
3. **Защищенная операционная система** – это ОС, предусматривающая средства защиты от основных классов угроз безопасности. Защищенная ОС обязательно должна содержать средства разграничения доступа к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с ОС. Кроме того, защищенная ОС должна содержать средства противодействия преднамеренному 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, обеспечивающая достаточный уровень защищенности ОС. Адекватность политики безопасности определяется не только архитектурой ОС, но и ее конфигурацией, установленными программами и т.д. Существует два основных подхода к созданию защищённых 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 незащищенную ОС антивирусного пакета, системы шифрования и т.д**.** **Комплексный подход –** это подход, предполагающий внесение защитных функций в ОС на этапе проектирования ее архитектуры. При этом защитные функции являются неотъемлемой частью ОС. **Типичные атаки на ОС:** Сканирование фаловой системы, кража ключевой информации, подбор пароля, сборка мусора, превышение полномочий, программные закладки, жадные программы.
4. **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 снижает безопасность защищаемой сети (т.к. блокируется сквозное прохождение пакетов), возможность осуществления большого количества дополнительных проверок. **Недостатки:** относительно 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.

***Осталось на листок переписать теперь весь этот фарш***