**1. Дать определения: информация, защищаемая информация, угрозы безопасности информации, привести типы угроз.** Информация - необработанные сведения о чем независимо от видов их представления. Защищаемая информация - информация, принадлежащая лицам, подлежащая защите в соответствии с требованиями правовых норм. Угрозы безопасности информации — это некая совокупность факторов и условий, которые создают опасность в отношении защищаемой информации. Три основные угрозы безопасности:1. угроза конфиденциальности - возможность получения информации для лиц,которым она не предназначалась 2. Угроза целостности - это угроза в результате реализациикоторой, информация становится изменённой или уничтоженной. 3. Угроза отказа в обслуживании (угроза доступности) - угроза, реализация которой приведет к отказу в обслуживании клиентов, несанкционированному использованию ресурсов злоумышленником в своих усмотрениях.

**2. Дать определение безопасности информации, средство защиты информации, перечислить направления защиты информации.** Безопасность информации - это состояние защищенности информации, при котором обеспечены её конфиденциальность, общедоступность и целостность.Средства защиты информации - вещество, материал, ПО, техническое,техническое ПО предназначенное для защиты информацииОсновные направления защиты информации:1. Правовая защита информации2. Техническая защита информации3. Криптографическая защита информации4. Физическая защита информации - защита информации путем применения организационных мероприятий, которые ограничивают доступ к информации.

**3. Дать определение защиты информации от несанкционированного доступа, перечислить методы защиты от НСД.** Защита от НДС - защита направленная на предотвращения получения защищённой информации заинтересованными пользователямиМетоды защиты от НДС:1. Идентификация - процесс присвоения пользователю уникальных имен или методов.2. Аутентификация - установление подлинности, проверка принадлежности пользователя предъявленного им идентификатора или данных.3. Управление доступом - метод защиты информации путём регулирования использования всех ресурсов системы.Три основных методов аутентификации:1. Аутентификация по наличию уникального ID2. Пользователю доступна и известна некоторая конфиденциальная информация (пароль)3. Аутентификация пользователя по каким-то персональным признакам (биометрическая)

**4. Парольные системы аутентификации. Основные понятия. Перечислить рекомендации для парольных систем.** Система где для аутентификации используется пароль, называются *парольной системой аутентификации.* *Идентификатор пользователя* -уникальная информация позволяющая различить отдельных пользователей друг от друга. *Пароль пользователя* - секретная информация известная только пользователю, которая используется для прохождения аутентификации. *Учетная запись пользователя* - совокупность идентификатора, пароля и возможной дополнительной информации. *Рекомендации:* 1) Установление минимальной длины пароля.2) Увеличение мощности алфавита паролей. 3) Проверка и отбраковка паролей по словарю.4) Установка минимального срока действия пароля. 5) Отбраковка по журналу истории паролей.6) Ограничение числа попыток ввода пароля. 7) Принудительная смена пароля при первом входе пользователя в систему. 8) Задержка при вводе неправильного пароля. 9) Запрет на выбор пароля пользователем и автоматическая генерация пароля.

**5: Модели безопасности. Определение, назначение, виды. Дискреционная модель безопасности. Привести примеры дискреционной модели безопасности.**

Модель безопасности - система, функционирующая в соответствии со строго определенным набором формализованных правил, и реализующие какую-либо политику безопасности

Модель безопасности включает: модель компьютерной (информационной) системы; критерии, принципы, ограничения и целевые функции защищенности информации от угроз; формализованные правила, ограничения, алгоритмы, схемы и механизмы безопасного функционирования системы. Целью этой модели является выражение сути требований по безопасности к данной системе. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации. Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты.

Виды: Модель дискреционного доступа (DAC) Модель безопасности Белла—ЛаПадулы(модель мандатного управления доступом). Ролевая модель контроля доступа (RBAC) В рамках дискреционной модели контролируется доступ субъектов (пользователей или приложений) к объектам (представляющим собой различные информационные ресурсы: файлы, приложения, устройства вывода и т.д.). Для каждого объекта существует субъект-владелец,который сам определяет тех, кто имеет доступ к объекту, а также разрешенные операции доступа. Основными операциями доступа являются READ (чтение), WRITE (запись) и EXECUTE (выполнение, имеет смысл только для программ). Таким образом, в модели дискреционного доступа для каждой пары субъект-объект устанавливается набор разрешенных операций доступа. Недостаток модели DAC заключается в том, что субъект, имеющий право на чтение информации может передать ее другим субъектам, которые этого права не имеют, без уведомления владельца объекта.

**6. Модели безопасности. Определение, назначение, виды. Мандатная модель. ЧАСТЬ В ПЯТОМ ВОПРОСЕ!** Модель мандатного управления доступом в основном известна двумя основными правилами безопасности: одно относится к чтению, а другое – к записи данных. Общее правило звучит так: пользователи могут читать только документы, уровень секретности которых не превышает их допуска, и не могут создавать документы ниже уровня своего допуска. То есть теоретически пользователи могут создавать документы, прочесть которые они не имеют права. Модель полностью формализована математически. Основной упор в модели делается на конфиденциальность, но кроме неё фактически больше ничего не представлено. «Сведения о том, что самолет несет груз из некоторого количества бомб, возможно, имеют более высокий уровень секретности, чем уровень доступа диспетчера, но диспетчеру тем не менее необходимо знать вес груза.»

**7. Модели безопасности. Определение, назначение, виды. Ролевая модель безопасности. Привести примеры ролевой модели безопасности. ЧАСТЬ В ПЯТОМ ВОПРОСЕ!** Ролевой метод управления доступом контролирует доступ пользователей к информации на основе типов их активностей в системе (ролей). Под ролью понимается совокупность действий и обязанностей, связанных с определенным видом деятельности. Примеры ролей: администратор базы данных, менеджер, начальник отдела. В ролевой модели с каждым объектом сопоставлен набор разрешенных операций доступа для каждой роли. В свою очередь, каждому пользователю сопоставлены роли, которые он может выполнять.1.Простота администрирования. В отличие от модели DAC нет необходимости прописывать разрешения для каждой пары «объект-пользователь». Вместо этого прописываются разрешения для пар «объект-роль» и определяются роли каждого пользователя. 2.Принцип наименьшей привилегии. Ролевая модель позволяет пользователю регистрироваться в системе ролью, минимально необходимой для выполнения требуемых задач. 3. Разделение обязанностей. RBAC широко используется для управления пользовательскими привилегиями в пределах единой системы или приложения. Список таких систем включает в себя Microsoft Active Directory, SELinux, СУБД, PostgreSQL и множество других, эффективно применяющих RBAC.

**8. Национальная безопасность РФ. Основные понятия и документы, определяющие национальную безопасность РФ.** Национальная безопасность - состояние защищенности личности, общества, государства от внешних и внутренних угроз, которые позволяют обеспечитьконституционные права, качества жизни, оборону и безопасностьУгроза национальной безопасности - совокупность условий и факторов, препятствующих реализации национальных интересов, а также создающих опасность национальным ценностям и национальному образу жизни.Cтратегические национальные приоритеты - важнейшие направления обеспечения национальной безопасности, по которым реализуются конституционные права и свободы граждан Российской Федерации.Система обеспечения национальной безопасности — это совокупность государственных и общественных институтов, действующих в интересах достижения необходимого уровня защищенности личности, общества и государства в различных сферах жизнедеятельности.Силы обеспечения национальной безопасности - Вооруженные Силы Российской Федерации, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба, а также федеральные органы государственной власти, принимающие участие в обеспечении национальной безопасности государства на основании законодательства Российской Федерации

**9.Понятие критически важного объекта. Классификация КВО. Критерии КВО, определяемые в других странах (США).** Крит. важный объект - объект, который оказывает сильное влияние на страну, прекращение работы которого приводит к чрезвычайной ситуации в стране.Классификация по значимости1. Федеральный уровень:2. Субъектовый уровень:3. Территориальный и муниципальный уровни:Классификация критически важных объектов по видам угроз• ядерно-опасные (атомные электростанции);• радиационно-опасные (места хранения жидких радиоактивных отходов, и др.);• химически-опасные (предприятия нефтехимического производства, пищевой пром);• биологически-опасные (предприятия по производству, переработке и хранению сельхозпродукции, и др.);• техногенно-опасные (крупные железнодорожные узлы, морские порты, аэропорты в крупных городах);• пожаро-взрывоопасные (магистральные газо-, нефте- и продуктопроводы, газокомпрессорные и нефтеперекачивающие станции);· объекты государственного управления, финансово-кредитной, информационной и телекоммуникационной инфраструктуры - узлы телефонной, телевизионной, архивы.Классификация критически важных объектов по уровням угроз1 класс - возникновения федеральных и/или трансграничных ЧС;2 класс - возникновения региональных ЧС;3 класс - возникновения территориальных ЧС;4 класс - возникновения местных ЧС;5 класс - возникновения локальных ЧС.

**10. Ключевая система информационной инфраструктуры. Состав КСИИ.** Ключевая система информационной инфраструктуры (КСИИ) - это информационно-управляющая или информационно телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан, и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация, или будут нарушены выполняемые системой функции управления со значительными негативными последствиями. Основным признаком принадлежности объекта к критически важным является наличие на объекте экологически опасного или социально значимого производства или технологического процесса, нарушение штатного режима которого приводит к чрезвычайной ситуации определенного уровня и масштаба, а также наличие на объекте информационной системы (элементов системы), которая осуществляет функции управления чувствительными (важными) для Российской Федерации процессами и нарушение функционирования которой приводит к значительным негативным для страны последствиям.К критически важным объектам относятся:· системы органов власти;· система органов управления правоохранительных структур;· системы финансово-кредитной и банковской деятельности;· системы предупреждающей и ликвидирующей чрезвычайной ситуации;· системы управления водоснабжения;· системы управления электроснабжения и др.

**11. Концепция деятельности ВС РФ в информационном пространстве.**

Принципы: законности, приоритетности, комплексности, взаимодействия, сотрудничества, инновационности. Деятельность вооруженных сил в информационном пространстве – использование вооруженными силами информационных ресурсов для решения задач обороны и безопасности. Информационная безопасность вооруженных сил - состояние защищенности информационных ресурсов вооруженных сил от воздействия информационного оружия. Информационная война - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны. Информационная инфраструктура - совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации. Информационное оружие - информационные технологии, средства и методы, применяемые в целях ведения информационной войны. Информационное пространство - сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию. Информационные ресурсы - информационная инфраструктура, а также собственно информация и ее потоки. Кризисная ситуация – этап эскалации конфликта, характеризующийся применением военной силы для его разрешения. Международная информационная безопасность - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве. Система обеспечения информационной безопасности Российской Федерации – часть системы обеспечения национальной безопасности страны, предназначенная для реализации государственной политики в сфере информационной безопасности.

**12. Криптографическая защита информации. Основные понятия. Общая схема криптосистем.** Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетяхКриптография представляет собой совокупность методов преобразования данных , направленных на то, чтобы защитить эти данные, сделав их бесполезнымиОсновой большинства криптографических средств защиты информации является шифрование данных.Под шифром понимают совокупность процедур и поавид криптографических преобразования, используемых для зашифроваия и расшифрования информации по ключу шифрованияШифр - это совокупность процедур и правил криптографических преобразований, используемых для зашифрования и расшифрования информации по ключу шифрованияКлюч шифрования - является элементом с помощью которого можно варьировать результат криптографического преобразования.Данный элемент может принадлежать конкретному пользователю или группе пользователей и является для них уникальным.Под шифрование информации понимается процесс преобразования открытой информации (исх. текста) и зашифрованный текст (шифртекст).Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют расшифровками (дешифрования)**.**

**13. Определение криптографии. Классификация криптоалгоритмов защиты информации.** Криптография-совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными.*Классификация:*2. Криптография с ключом. Алгоритм воздействия на передаваемые данные известен всем сторонним лицам, но он зависит от некоторого параметра – "ключа", которым обладают только отправитель и получатель.1. Симметричные криптоалгоритмы.Для зашифровки и расшифровки сообщения используется один и тот же блок информации (ключ).2. Асимметричные криптоалгоритмы.Алгоритм таков, что для зашифровки сообщения используется один ("открытый") ключ, известный всем желающим, а для расшифровки – другой ("закрытый"), существующий только у получателя.В зависимости от характера воздействий, производимых над данными, алгоритмы подразделяются на:1. ПерестановочныеБлоки информации (байты, биты, более крупные единицы) не изменяются сами по себе, но изменяется их порядок следования2. Подстановочные.Сами блоки информации изменяются по законам криптоалгоритма (их больше всего).В зависимости от размера блока информации криптоалгоритмы делятся на:1. Потоковые шифры.Единицей кодирования является один бит. Результат кодирования не зависит от прошедшего ранее входного потока. Схема применяется в системах передачи потоков информации, то есть в тех случаях, когда передача информации начинается и заканчивается в произвольные моменты времени и может случайно прерываться. Блочные шифрыЕдиницей кодирования является блок из нескольких байтов. Результат кодирования зависит от всех исходных байтов этого блока. Схема применяется при пакетной передаче информации и кодировании файлов

**14. Симметричное шифрование. Основные алгоритмы. Принцип работы.** *Симметричное шифрование* - это метод шифрования, при котором для защиты информации используется ключ, зная который любой может расшифровать или зашифровать данные. Высокая стойкость. Так как для шифрования и дешифрования используется один и тот же ключ, при использовании таких алгоритмов требуются высоко надежные механизмы для распределения ключей.Проблема: является безопасное распространение симметричных ключей. Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных. *Гаммированием* (gamma xoring) называется процесс «наложения» гамма-последовательности на открытые данные. Обычно это суммирование по какому-либо модулю. В симметричном шифровании, основанном на использовании составных ключей, идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Каждая часть сама по себе не позволяет выполнить дешифрование. Основным *недостатком* симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. Это создает проблему распространения ключей. Получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно. *Алгоритмы:* DES (56 бит, шифрование (перестановками через сеть Фейстеля) в 16 раундов+ 2 перестановки (начальн и конечн), на каждом раунде вкидывается частичный ключ в то, что шифруется)., AES(блочное шифрование, ключ на 128, 192 или 256 бит), ГОСТ 28147-89 - советский и российский стандарт шифрования, RC4 ()- применяется в протоколах SSL, TSL, в обеспечении безопасности беспроводных сетей WEP, WPA, IDEA (Internatioanl Data Encryption Algorithm)- международный алгоритм шифрования данных, Kuznechik (ГОСт Р. 34.12.2015) (256 бит-длина ключа, через подстановки, их 10 штук, но последняя –неполная (там только часть алгоритма выполняется).

**15. Асимметричное шифрование. Основные алгоритмы. Принцип работы.** Асимметричный алгоритм предполагает под собой наличие двух ключей — публичного и приватного. То есть сообщение шифруется публичным ключом, а расшифровывается приватным и ни как иначе. Собственно именно эту концепцию сформулировал Диффи.В общем суть данного алгоритма заключается в том, что принимающая сторона перед приемкой сообщения генерирует пару ключей на основе алгоритма модульной арифметики (принцип такой же как и в алгоритме Диффи-Хеллмана), собственно приватный и публичный ключ. Отправитель перед отправкой получает публичный ключ и шифрует сообщение данным ключом, после чего данное сообщение можно расшифровать только приватным ключом, который хранится в секрете у принимающей стороны.Асимметричные криптосистемы шифрования.RSA(Через перемножение и функцию эйлера)DSA(криптографический алгоритм с использованием открытого ключа для создания электронной подписи, но не для шифрования. Только один субъект может создать подпись сообщения, но любой может проверить её корректность.) Алгоритм основан на вычислительной сложности взятия логарифмов в конечных полях.)ГОСТ Р 34.10-2012RSA - предложили в 1978 года три автора: Р. Райвест, А. Шамир, А. Адлеман

**16. Понятие и предмет форензики.** Форензика (компьютерная криминалистика) является прикладной наукой о раскрытии и расследовании преступлений, связанных с компьютерной информацией, о методах получения и исследования доказательств, имеющих форму компьютерной информации (так называемых цифровых доказательств), о применяемых для этого технических средствах.Сферы применения форензики:1. Раскрытие и расследование уголовных преступлений, в которых фигурируют комп информации2. Сбор и исследование доказательств для гражданских дел3. Страховые расследования проводимые страховыми компаниями4. Внутрикорпоративные расследования инцидентов безопасности5. Военные и разведывательные задачи по поиску уничтожению и восстановлению компьютерной информации в ходе оказания воздействия на информационные системы противника и защиты своих систем.Предметами форензики являются:· криминальная практика – способы, инструменты совершения соответствующих преступлений, их последствия, оставляемые следы, личность преступника;· оперативная, следственная и судебная практика по компьютерным преступлениям;· методы экспертного исследования компьютерной информации и, в частности, программ для ЭВМ;· достижения отраслей связи и информационных технологий (ИТ), их влияние на общество, а также возможности их использования как для совершения преступлений, так и для их предотвращения и раскрытия.

**17. Личность вероятного преступника. Определение. Основные типы.**

Уровень компетенции в ИТ важен. Когда квалификация подозреваемого неизвестна, ее следует предполагать высокой. С той же целью специалисту или следователю имеет смысл до поры скрывать свой собственный уровень познаний в ИТ перед подозреваемым. «Хакер». Мотивация: исследовательский интерес, любопытство, стремление доказать свои возможности, честолюбие. Средства защиты компьютерной информации, ее недоступность они воспринимают как вызов своим способностям. Наряду с многознающими «хакерами» вводят отдельную категорию «script kiddies\*». Это те, кто движим теми же мотивами, но не в состоянии придумать свое и поэтому просто бездумно используют готовые инструменты, сделанные другими. Основные черты: интровертность, Эскапизм, сетевой аддикция, психической девиации, эмоциональной чувствительностью «Инсайдер» (наименование условное). Человек, не слишком хорошо владеющий знаниями в области ИТ, зато владеющий доступом в информационную систему (ИС) в силу служебного положения. Итак, типичный «инсайдер» совершает компьютерное преступление (лично или в форме подстрекательства, совместно с «внешним» соучастником) с использованием сведений, полученных в силу служебного положения.» «Белый воротничок». Этот тип преступника представляет собой давно и хорошо известного казнокрада, но только сменившего инструменты своей деятельности на компьютер В отличие от «инсайдера», этот тип злоумышленника имеет минимальную квалификацию в сфере ИТ и компьютер как орудие совершения преступления не использует По своим мотивам «белые воротнички» могут быть разделены на три группы: 1. Злоупотребляющие своим служебным положением из чувства обиды на компанию или начальство. 2. Беспринципные расхитители, не имеющие моральных барьеров и ворующие только потому, что представилась такая возможность. 3. Квазивынужденные расхитители, попавшие в тяжелое материальное положение, в материальную или иную зависимость от лица, требующего совершить хищение или мошенничество. «Е-бизнесмен». Этот тип вероятного преступника не является квалифицированным ИТ-специалистом и не имеет служебного положения, которым можно злоупотребить. С самого начала он планирует именно криминальное предприятие, отлично осознаёт его противозаконность. Решение совершить правонарушение именно в компьютерной (сетевой) среде, а не в офлайне\* он принял не из-за своих особых знаний в этой области и не из-за внутренней тяги к компьютерам, а исключительно на основе рационального анализа «Выгода» компьютерного преступления обычно связана с его технической или организационной сложностью. «Антисоциальный тип». Также отмечались интернет-мошенники, которые руководствовались не только извлечением прибыли. Более того, их преступный доход часто бывал меньше, чем средняя зарплата специалиста той же квалификации. Мотивом для совершения мошенничества являлась антисоциальная психопатия (социопатия) таких лиц и их патологическая тяга к ведению подобных «игр».

**18. Определение компьютерного преступления. Виды Компьютерных преступлений. Онлайн-мошенничество.** Компьютерное преступление - уголовное правонарушение для расследования которого существенным условием является применение специальных знаний в области информационных технологий.Виды компьютерных преступлений:· Взломo Получение несанкционированного доступа к данным, через компьютерные системы называется взломом. · Фишинг**-**попытка завладеть конфиденциальной информацией, такой как имена пользователей, пароли и данные кредитной карты, которая выглядит как источник, заслуживающий доверия. · Компьютерные вирусыo Компьютерные вирусы - Компьютерные вирусы-это формы вредоносных кодов, написанных с целью нанесения вреда компьютерной системе и уничтожения информации. · Киберпреследованиеo Использование коммуникационных технологий, главным образом Интернета, с целью преследования лиц, известно, как киберпреследование.· Кибервымогательствоo Когда злоумышленники угрожают или вредят веб-сайту, серверу или компьютерной системе с помощью отказа в обслуживании (DOS) или других атак на уязвимую систему с целью шантажа · Электронный спамo Это относится к использованию электронных систем обмена сообщениями для отправки нежелательных сообщений пользователям. · Киберсквоттингo регистрация доменных имён, содержащих торговую марку, принадлежащую другому лицу с целью их дальнейшей перепродажи или недобросовестного использования. Онлайн-мошенничество (Fraud) - действия киберпреступников направленные на овладение информационными данными или финансовыми средствами пользователя интернет.Классификация:1. "Нигерийские письма" - сначала чуть-чуть отправишь потом получишь доходы2. Ошибочный платёж - перевели тебе попросили вернуть, ты перевёл обратно, а в это время с той стороны отменяют перевод3. Заграничная невеста - невесте нужны деньги на переезд4. Письма счастья - вы выиграли миллион !5. Фишинговые сайты - копия популярного сайта6. Лжеблокировка счета7. Ложный покупатель - скажи cvv карты на которую перевести деньгиАнализ риска онлайн-мошенничества:1. Видимая сильная экономия2. Стремление скрыть личность3. Только безналичная оплата

**19. Определение компьютерного преступления. Виды Компьютерных преступлений. Нежелательный контент. ЧАСТЬ В 18 ВОПРОСЕ!!!** Нежелательный контент – это не только материалы (картинки, видео, аудио, тексты), содержащие насилие, порнографию, пропаганду наркотических средств, азартных игр, но и различные компьютерные вирусы, шпионские программы, задача которых получить доступ к информации на компьютере владельца. Также к нежелательному контенту относятся сайты, запрещенные законодательством. Классификация нежелательного контента: · Вредоносные программы · Спам · Потенциально опасные программы · Запрещенные законодательством · Нежелательные сайты

**20. Определение компьютерного преступления. Виды Компьютерных преступлений. ЧАСТЬ В 18 ВОПРОСЕ!!!** Распределенные атаки на отказ в обслуживании. DoS (от англ. Denial of Service — отказ в обслуживании) — хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. Классификация атак Первый класс (L2) — ICMP Flood «забивание» канала. Это атаки, которые направлены на лишение доступа к внешней сети вследствие исчерпания канальной ёмкости. Абсолютно неважно, каким именно образом. Как правило, для этой цели используются массированные, с точки зрения трафика, атаки типа «что-нибудь»-Amplification (NTP-, DNS-, RIP-… Amplification может быть любой, не имеет смысла перечислять). Второй класс (L3) — вероятно UDP Flood, нарушение функционирования сетевой инфраструктуры. К этому классу относятся, в числе прочего, атаки, приводящие к проблемам с маршрутизацией в рамках протокола BGP, с анонсами сетей (Hijacking) — или атаки, следствием которых становятся проблемы на транзитном сетевом оборудовании: например, переполнение таблицы отслеживания соединений. Третий класс (L4) — SYN Flood эксплуатация слабых мест TCP-стека, то есть атаки на транспортном уровне. Этот транспортный протокол, лежащий в основе HTTP и ряда других протоколов, довольно сложно устроен. Например, в нём используется большая таблица открытых соединений, каждое из которых является, фактически, конечным автоматом. И именно атаки на этот автомат составляют третий класс DDoS-нападений. Четвёртый класс (L7) — HTTP Flood, деградация Web-приложения. Сюда относятся всевозможные «кастомные» атаки, начиная от типичного GET/POST/HTTP Flood до нападений, нацеленных на многократно повторяющиеся поиск и извлечение конкретной информации из БД, памяти или с диска, пока у сервера просто не закончатся ресурсы.

**21. Определение компьютерного преступления. Виды Компьютерных преступлений. Дефейс. ЧАСТЬ В 18 ВОПРОСЕ!!!** *Компьютерное преступление* - уголовное правонарушение для расследования которого существенным условием является применение специальных знаний в области информационных технологий. *Виды компьютерных преступлений:* Взлом*,* Фишинг*,* Компьютерные вирусы*,* Киберпреследование*,* Кибервымогательство*,* Электронный спам*,* Киберсквоттинг.

Deface (англ. deface — уродовать, искажать) — тип хакерской атаки, при которой главная (или другая важная) страница веб-сайта заменяется на другую — как правило, вызывающего вида (реклама, предупреждение, угроза…). Зачастую доступ ко всему остальному сайту блокируется, или же прежнее содержимое сайта вовсе удаляется.

**22. Определение компьютерного преступления. Виды Компьютерных преступлений. Вредоносные программы. ЧАСТЬ В 18 ВОПРОСЕ!!!** *Компьютерное преступление* - уголовное правонарушение для расследования которого существенным условием является применение специальных знаний в области информационных технологий. *Виды компьютерных преступлений:* Взлом*,* Фишинг*,* Компьютерные вирусы*,* Киберпреследование*,* Кибервымогательство*,* Электронный спам*,* Киберсквоттинг.

*Вредоносная программа* (Malware) - программное обеспечение, разработанное специально для нанесения вреда компьютеру. Чаще всего, такое вредительство осуществляется несанкционированным проникновением в компьютер пользователя, целью которого может быть воровство личных данных, уничтожение файлов, внесение изменений в регистры, нарушающие нормальную работу операционной системы и многие другие преступные действия. Подвиды троянов: SpyWare - предназначены для похищения персональных данных, AdWare - предназначены для скрытной демонстрации пользователю несанкционированной рекламы, RAnsonWare - блокировка файлов.

**23. Определение компьютерного преступления. Виды Компьютерных преступлений. Мошенничество с платежными картами. ЧАСТЬ В 18 ВОПРОСЕ!!!** Неск видов: получение - распределение – реализация. На первом этапе данные о банковских картах получают разнообразными способами. На втором этапе они сортируются, проверяются, классифицируются. На третьем этапе данные банковских карт реализуются, то есть конвертируются в деньги. Указанная цепочка никогда не исполняется одним человеком. Каждый из этапов связан со своими особенными навыками, опытом в соответствующей области, служебным положением, доступом к технике. Поэтому криминальная цепочка всегда включает не менее трёх сообщников. Наборы данных банковских карт, которые представляют ценность: 1) номер, срок действия, имя владельца, код cvv или cvv2 2) дамп карты (копия содержимого магнитной полосы карты) 3) дамп + пин-код Способы получения данных банковских карт: дистанционный, доступ к таким данным с использованием своего служебного положения, перехват интернет-трафика, получение данных банковских карт, или снятие дампа при обслуживании клиентов в предприятиях торговли и питания - похож на предыдущий способ, но особенность в том, что информация копируется непосредственно с карты при физическом контакте с ней; - выманивание данных карт и иногда пин-кодов у владельцев методами фишинга; - получение дампов и пин-кодов при помощи фальшивых банкоматов или приставок к банкоматам (скиминг); - получение самой карточки мошенническим способом ("ливанская петля" и др.); - обычная кража карты у её держателя (бывает, что пин-код записан на ней или на листке, лежащем в том же бумажнике).

**24. Определение компьютерного преступления. Виды Компьютерных преступлений. Нарушение авторских прав. ЧАСТЬ В 18 ВОПРОСЕ!!!** Нарушение авторских прав:Нарушение авторских прав подразумевает не санкционированное правообладателем распространение материала, защищённого авторским правом, такого, как программное обеспечение, музыкальные композиции, фильмы, книги, компьютерные игры.Под нарушением авторских прав обычно понимаются следующие действия:· создание копии и её продажа;· создание копии и передача её кому-либо ещё;· в некоторых случаях перепродажа легально приобретённой копии.

**25. Определение компьютерного преступления. Виды Компьютерных преступлений. Фишинг. ЧАСТЬ В 18 ВОПРОСЕ!!!** Фишинг (Phishing) - это почтовая рассылка имеющая своей целью получение конфиденциальной финансовой информации. Такое письмо, как правило, содержит ссылку на сайт, являющейся точной копией интернет-банка или другого финансового учреждения. Пользователь, обычно, не догадывается, что находится на фальшивом сайте и спокойно выдает злоумышленникам информацию о своих счетах, кредитных карточках, паролях и т. д.

**26. Определение компьютерного преступления. Виды Компьютерных преступлений. Киберсквоттинг. ЧАСТЬ В 18 ВОПРОСЕ!!!** Киберсквоттингрегистрация доменных имён, содержащих торговую марку, принадлежащую Виды· Тайпсквоттинг — регистрация доменных имён, близких по написанию с адресами популярных сайтов, в расчёте на ошибку части пользователей. Например, «wwwsite.ru» в расчёте на пользователя, который хотел попасть на «www.site.ru». При близости к очень популярным доменам · Брендовый киберсквоттинг — регистрация доменных имён, содержащих товарные знаки, фирменные наименования, популярные имена собственные, то есть средства индивидуализации, охраняемые законом, а также регистрация «на перспективу», например, создатель фильма «ABC» регистрирует сайт «ABC.com», а киберсквоттер, с надеждой, что выйдет продолжение фильма, постарается сразу зарегистрировать на себя «ABC2.com», «ABC3.com», «ABC4.com» и т. д. · Защитный киберсквоттинг — когда легальный владелец непопулярного сайта (товарного знака) регистрирует все доменные имена, близкие, созвучные, похожие, связанные по смыслу с его собственным доменным именем. Делается для того, чтобы не стать жертвой киберсквоттеров. Например, владелец популярного сайта «www.firma.ru» может захотеть также зарегистрировать домены «firma-msk.ru», «firma-spb.ru» и «firma.org», чтобы перенаправлять с них посетителей на свой основной сайт, а также «anti-firma.ru», чтобы недоброжелатели не смогли использовать его.Бывают случаи, когда доменное имя захватывают с целью шантажа или вымогательства. Киберсквоттер угрожает разместить на захваченном домене сайт с негативной информацией или выдавать этот сайт за принадлежащее правомерному владельцу средство индивидуализации.

**27. Технические средства из состава Kali Linux. Перечислить основные инструменты, дать определения.** · Aircrack-ng - набор программ, предназначенных для обнаружения беспроводных сетей, перехвата передаваемого через беспроводные сети трафика, аудита WEP и WPA/WPA2-PSK ключей шифрования (проверка стойкости), в том числе пентеста (Penetration test) беспроводных сетей (подверженность атакам на оборудование и атакам на алгоритмы шифрования).· Burp Suite – это платформа для проведения аудита безопасности веб-приложений. Содержит инструменты для составления карты веб-приложения, поиска файлов и папок, модификации запросов, фаззинга, подбора паролей и многое другое.· Ettercap — это утилита для анализа сетевого трафика, проходящего через интерфейс компьютера, но с дополнительной функциональностью. Программа позволяет выполнять атаки типа «Человек посередине» чтобы заставить другой компьютер передавать пакеты не маршрутизатору, а пользователю Ettercap.· Hydra - инструмент для анализа безопасности компьютерной сети, обладающий большим количеством разнообразных возможностей, особо популярным за умение выполнять ARP-spoofing.· John the Ripper - Свободная программа, предназначенная для восстановления паролей по их хешам. Основное назначение программы - аудит слабых паролей в UNIX системах путем перебора возможных вариантов.· Maltego - это программа, которая проводит сбор информации на основе разнообразных сканирований, в том числе сканирований на наличие документов с метаданными, сканирований уязвимостей, программа анализирует полученную информацию и графически отображает собранные данные.· Kismet - это детектор беспроводных сетей 802.11, сниффер и система выявления вторжений.· Metasploit - инструмент для создания, тестирования и использования эксплойтов.· Nmap - утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб)· OWASP-ZAP - это простой в использовании интегрированный инструмент тестирования на проникновения и нахождения уязвимостей в веб-приложениях.· sqlmap — это инструмент для тестирования на проникновение, который автоматизирует процесс выявления и эксплуатации уязвимости SQL-инъекцй и захват серверов баз данных.· Wireshark - программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других· Reaver - Инструмент позволяющий провести атаку на WiFi роутер, основанную на уязвимости WPS путём Брутфорса 8-значного числа. И позволяющий получить WiFi пароль от роутера.

**28. Понятие анонимности в интернете. Виды анонимности. Средства обеспечения анонимности.** Сетевая анонимность - состояние, в котором невозможно установить личность автора в сети.Финансовая анонимность - состояние, при котором невозможно установить личность при совершении финансовой операции.Анонимность в медицинеАнонимность в благотворительностиСредства обеспечения анонимности:Прокси-серверы - Промежуточный сервер в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером, позволяющийклиентам как выполнять косвенные запросы к другим сетевым службам, так и получать ответыVPN - Обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети.SHH - Сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.Tor — свободное и открытое программное обеспечение для реализации второго поколения так называемой луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

**29. Персональные данные. Определение. Закон РФ о персональных данных. Основные понятия федерального закона.** Персональные данные - это любая информация, относящаяся прямо или косвенно определенному, или определяемому лицуФЗ №152 "О персональных данных"Основные понятия:· Оператор - государственный орган самостоятельно или совместно с другими организациями организующий обработку или хранение персональных данных, а также определяющий цели обработки персональных данных· Обработка персональных данных - совокупность действий совершаемых с использованием средств автоматизации. Включая сбор, запись, систематизацию, накопление,хранение, уточнение, использование, блокирование и уничтожение персональных данных.· Автоматизированная обработка персональных данных - обработка персональных данных с использованием автоматизации.· Распространение персональных данных - раскрытие персональных данных неопределенному кругу лиц.· Предоставление персональных данных - раскрытие персональных данных определенному кругу лиц.· Блокирование персональных данных - Временное прекращение обработки персональных данных.· Уничтожение персональных данных - это действие, в результате которого невозможно определить или использовать персональные данные, в результате, которых уничтожается материальные или нематериальный носители.· Обезличивание персональных данных - действие, в результате которых становится невозможно без использования дополнительной информации определить, кому принадлежат данные· Трансграничная передача персональных данных - это передача данных на территорию иного государства, органы власти иностранного государства,иностранному физ/юр. лицу.

**30. Персональные данные. Определение. Принципы и условия обработки персональных данных.** Персональные данные - это любая информация, относящаяся прямо или косвенно определенному, или определяемому лицуПринципы:1. Законность и справедливость2. Достижение конкретных целей3. Несовместимость данных4. Минимизация данных5. Отсутствие избыточности 6. Точность, достаточность и актуальность данных7. Соблюдение сроков храненияУсловия:1. Согласие субъекта2. В соответствии с международным договором3. Исполнение судебного акта4. Предоставление государственных и муниципальных услуг5. Договор с субъектом6. Защита жизни и здоровья субъекта7. Осуществление прав и законных интересов оператора8. Статистические или иные исследования9. Профессиональная деятельность10. Просьба субъекта11. В соответствии с ФЗ

**31. Персональные данные. Определение. Защита персональных данных.** Персональные данные - это любая информация, относящаяся прямо или косвенно определенному, или определяемому лицуДля выполнения требований закона "О персональных данных" оператор персональных проводите следующие организационные и технические мероприятия:- Уведомление уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществить обработку персональных данных- Разработка документов, регламентирующих обработку ПД в организации (положение по обработке персональных данных, регламенты и т.п.)- Создание системы защиты ПД, в т.ч. выполнение требований по инженерно-технической защите помещений- Аттестация или декларирование соответствия информационной системы персональных данных требованиям безопасности информации- Повышение квалификации сотрудников в области защиты ПД

**32. Методы использования интернета в террористических целях.** 1. Пропаганда– вербовка– подстрекательство– радикализация2. Финансирование3. Подготовка террористов4. Планирование- секретная связь в процессе подготовки- Общедоступная информация5. Исполнение6. Кибератаки

**33. Программное обеспечение. Определение. Классификация. Этапы жизненного цикла программного обеспечения.** ПО - это совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.Классификация:По способу исполнения программ:· интерпретируемые· компилируемыеПо степени переносимости:· платформозависимые· кроссплатформенныеПо способу распространения и использования:· несвободные (закрытые)· открытые· свободныеПо назначению программы делятся на :· системные· прикладные· инструментальныеПо видам:· компонент· комплексЭтапы жизненного цикла ПО:1. Формулирование требований2. Проектирование3. Реализация 4. Тестирование5. Эксплуатация и сопровождение

**34. Ошибки и уязвимости программного обеспечения. Привести примеры. Общая классификация уязвимостей.** Дефект(ошибка) - это всё, что требует внесения изменений в разрабатыватываемый продукт.Уязвимость - дефект, который может быть использован для нарушения безопасности информацииЭксплойт - программы, с помощью которых производится эксплуатация уязвимостей.Примеры дефектов в С/C++ :· Утечка динамической памяти· Утечка дескрипторов· Множественное освобождение дескриптора· Множественное освобождение памяти· Неполное освобождение памяти· Освобождение памяти для указателя на статический объект· Разыменование нулевого или неинициализированного указателя· Использование неинициализированной переменной· Переполнение буфера· Деление на ноль· Вычитание и сравнение указателей на разные объекты· Переполнение буфера при строковых операциях· Ошибки форматной строкиОбщая классификация уязвимостей: · Php инъекции· Межсайтовая подделка запросов· Межсайтовый скриптинг· Внедрение sql кода

**35. Классификация уязвимостей OWASP. Уязвимость SQL-инъекций.** *OWASP*- Open Web Application Security Project — открытый проект обеспечения безопасности веб-приложений*. Классификация:* ·Внедрение кода, Некорректная аутентификация и управление сессией, Межсайтовый скриптинг (XSS), Небезопасные прямые ссылки на объекты, Небезопасная конфигурация, Утечка чувствительных данных, Отсутствие контроля доступа к функциональному уровню, Подделка межсайтовых запросов (CSRF), Использование компонентов с известными уязвимостями, Невалидированные редиректы. *SQL-инъекция* используется для атаки веб-сайтов, работающих с базами данных. *Возможность внедрения SQL-кода* возникает, если в SQL-запросах используются неотфильтрованные данные, вводимые пользователями. SQL-запросы используются для извлечения информации из базы данных, добавления информации в базу данных, а также для изменения и удаления данных в базе. Многие современные веб-сайты используют скрипты и SQL для динамического формирования содержимого страницы. В SQL-запросах часто используются данные, вводимые пользователями; это может привести к угрозе безопасности, поскольку хакеры могут попытаться внедрить во входные данные вредоносный SQL-код. Без надлежащих мер защиты такой код может быть успешно выполнен на сервере.

**36. Классификация уязвимостей OWASP. Уязвимость XSS-инъекций.**

*OWASP*- Open Web Application Security Project — открытый проект обеспечения безопасности веб-приложений*. Классификация:* ·Внедрение кода, Некорректная аутентификация и управление сессией, Межсайтовый скриптинг (XSS), Небезопасные прямые ссылки на объекты, Небезопасная конфигурация, Утечка чувствительных данных, Отсутствие контроля доступа к функциональному уровню, Подделка межсайтовых запросов (CSRF), Использование компонентов с известными уязвимостями, Невалидированные редиректы.

XSS ( Cross-Site Scripting — «межсайтовый скриптинг») — тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника. *Два типа уязвимостей*. Активная уязвимость более опасна, поскольку злоумышленнику нет необходимости заманивать жертву по специальной ссылке, ему достаточно внедрить код в базу или какой-нибудь файл на сервере. Таким образом, все посетители сайта автоматически становятся жертвами. Он может быть интегрирован, например, с помощью внедрения SQL-кода (SQL Injection). Пример пассивной уязвимости: тут уже нужна социальная инженерия, например, важное письмо от администрации сайта с просьбой проверить настройки своего аккаунта, после восстановления с бэкапа (в результате-переход по ссылке).

**37. Определение уязвимости программного обеспечения. Методы поиска уязвимостей.** В компьютерной безопасности термин «уязвимость» используется для обозначения недостатка в системе, используя который можно намеренно нарушить её целостность и вызвать неправильную работу. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных программ, скриптовых и SQL-инъекций.Методы поиска:· Ручной поиск· Поиск по шаблонам – автоматизированный метод, основанный на сравнении некоторых характеристик исследуемого ПО с заранее подготовленными описаниями (сигнатурами) уязвимых мест. Данный метод эффективен при поиске несложных уязвимостей и немаскируемых закладок, таких как переполнение буфера, парольные константы и т.д.· Fuzzing - техника тестирования программного обеспечения, часто автоматическая или полуавтоматическая, заключающаяся в передаче приложению на вход неправильных, неожиданных или случайных данных. Предметом интереса являются падения и зависания, нарушения внутренней логики и проверок в коде приложения, утечки памяти, вызванные такими данными на входе. Фаззинг является разновидностьювыборочного тестирования, часто используемого для проверки проблем безопасности в программном обеспечении и компьютерных системах.

**38. Определение уязвимости программного обеспечения. Основные методы противодействия уязвимостям.** В компьютерной безопасности термин «уязвимость» используется для обозначения недостатка в системе, используя который можно намеренно нарушить её целостность и вызвать неправильную работу. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных программ, скриптовых и SQL-инъекций. Среди методов противодействия выделяются следующие основные группы: · правовые методы; · экономические методы; · организационные методы; · инженерно-технические методы; · технические методы; · программно-аппаратные методы. При выборе методов парирования угроз (защиты информации) учитываются полученные в ходе анализа коэффициенты опасности каждого источника угроз, уязвимости и коэффициенты групп методов реализации угроз ИБ.

**39. Обнаружение вредоносного программного обеспечения. Определение. Классификация. Сигнатурный анализ.** Детектирование - процесс определения антивирусным программным обеспечением исполняемого файла как вредоносного.Классификация:- Сигнатурный метод детектирования- Вероятностные методы, в которые в свою очередь входят:- эвристический анализ- поведенческий анализ Способы обнаружения вторжения: - Сетевой (основан на модели OSI) - Прикладной (основан на работе ОС), S = (V,P,T) {0,1}, V - размер участка сигнатур, P - смещение от которого надо искать сигнатуру, T – шаг. Сигнатурный анализ - он основан на поиске в файле определенных последовательностей байтов, называемых сигнатурами. Сопоставление их с имеющимися в базе сигнатурами известных вирусов и является основной такого метода.

Основным способом детектирования при использовании сигнатурного метода является сканирование файла. Во время сканирования файл не запускается. Процесс создания сигнатур Нахождение вредоносного ПО Анализ вредоносного ПО и извлечение сигнатуры Тестирование сигнатуры Обновление базы Плюсы и минусы сигнатурного метода детектирования

Плюсы: Высокая достоверность обнаружения вредоносных программ (почти 100%) Минусы:

- неспособность обнаружения новых ранее неизвестных вредоносных программ и компьютерных вирусов - трудоемкий процесс ручного анализа вредоносных программ и извлечения сигнатуры, что приводит к значительным временным затратам выпуска обновлений для новых угроз.

**40. Обнаружение вредоносного программного обеспечения. Определение. Классификация. Эвристический анализ. ЧАСТЬ В 39 ВОПРОСЕ!!!** Эвристический анализ в общем случае основан на статистической информации о виде, свойствах и поведении исполняемых файлов.

Минусы: - относительная сложность анализа ПО - нагрузка системы на исполняемые файлы - не гарантии обнаружения вредоносного ПО возможны ложные срабатывания.

**41.Обнаружение вредоносного программного обеспечения. Определение. Классификация. Поведенческий анализ. ЧАСТЬ В 39 ВОПРОСЕ!!!** Поведенческий анализ может происходить различными способами - с помощью драйверов, перехватывающих системные вызовы, с помощью мониторов, фиксирующих изменения файлов или настроек системы.

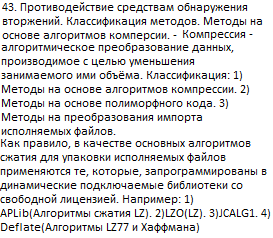
По завершению “ПА”, формируются признаки на предмет подозрительной деятельности. Для реализации этого подхода исполняемый файл запускается в режиме эмуляции в специальной среде антивирусов - "В песочнице". Какая-то формула: H = a: X->Y Xi э X -> fi D<fi> = Xi э X; Xi -> Yi D<fi> - пространство признаков, с помощью которых можно определить тип ПО (вредоносное или нет) Поведенческие блокираторы основаны на принципе перехвата всех подозрительных действий исполняемого файла и их блокировки, или запросе у пользователя разрешения на продолжение работы файла. В отличие от эвристического анализа, поведенческие блокираторы работают в реальной системе пользователя. Минусы: - относительная сложность их работы, нагрузка на систему, во время исследования - Нет 100% гарантии обнаружения вредоносного ПО, возможны ложные срабатывания.

**42. Классификация эвристических признаков вредоносного программного обеспечения.** Использование эвристик при извлечении признаковВ ходе работы было принято решение извлекать признаки 3-х видов:• Признаки, описывающие свойства PE формата.• Признаки, описывающие свойства файла, как простой последовательностибайт. • Эвристические признаки - попытка обобщения знаний о зловредных файлах врамках признаков. *Свойства PE формата*-Это признаки, опирающиеся на свойствах PE формата. Они призваны дать нам представление о структуре исполняемого файла. К ним относится всё, что касается информации, заключённой в PE заголовке, а также всего, на что он ссылается. *Свойства файла*

До сих пор мы рассматривали исполняемый файл с точки зрения структуры, продиктованной PE форматом. Но существует и другой подход. Мы можем относиться к исполняемому файлу как к простой последовательности байт фиксированной длины. Признаки из этой категории являются попыткой описать простейшие свойства файла, как упорядоченного массива байт. Сейчас мы будем рассматривать всего два из них – строки, входящие в состав файла, и размер файла. Строки. Строки, встречающиеся в файле,– один из наиболее часто используемых признаков при решении задачи классификации исполняемых файлов, В число строк входят все имена API функций и динамических библиотек, используемых файлом. А значит, строки дают нам представ ление о поведении файла в системе

*Признаки и эвристики* При извлечении признаков этого типа предполагается применение различных эвристик, полученных на основе знаний в предметной области. Эту группу признаков планируется активно пополнять новыми эвристиками для более успешной работы будущего классификатора исполняемых файлов. В данной работе мы рассмотрим несколько признаков и подробно обсудим причины, по которым эти признаки могут быть информативными.

**43. Противодействие средствам обнаружения вторжений. Классификация методов. Методы на основе алгоритмов компрессии.**



**44. Противодействие средствам обнаружения вторжений. Классификация методов. Методы на основе полиморфного кода.**

В настоящее время различают шесть степеней полиморфизма в соответствии с классификацией CARO(Computer Antivirus Research Organization): - Первый уровень полиморфизма использует постоянные значения для разных типов «стаба». - На втором уровне полиморфизма код «стаба» имеет постоянной одну или несколько инструкций. Могут использоваться различные регистры, некоторые альтернативные инструкции. - На третьем уровне полиморфизма в “стабе” используются команды, не участвующие в его работе, так называемые мусорные команды. Примером команд могут быть: - однобайтовые команды «МОР» - однобайтовые команды, манипулирующие с битами регистра флагов процессора «CLI», «SТD» и прочими; - однобайтовые команды, манипулирующие с неиспользуемыми в расшифрощике регистрами - “DEC DX”, “INC BP” и прочими; - однобайтовые префиксы переназначения сегментов «СS:», «DC» прочих; - многобайтовые и многокомандные комбинации, не выполняется никаких «полезных» действий, - пары «PUSH.POP» типа «пустышки” или «АРО АХО» и прочие; - «ложные» и «бессмысленные» условные и безусловные пер «JМР $+3» и прочие. - На четвертом уровне полиморфизма команды «стаба» могут быть заменены своими функциональными эквивалентами. Например, команд “MOV AX, 0” точно так же обнуляет регистр AX, как команда «SUB AX, AX» или пара команд «PUSH 0/POP AХ», - Пятый уровень полиморфизма включает свойства всех перечисленных уровней, а кроме того, в «стабе» могут применяться различные алгоритмы извлечения и исполнения основного кода скрываемого исполняемого файла. - Шестой уровень полиморфизма предусматривает перестановку с ме как отдельных команд, так и целых блоков исполняемого кода «стаба» уровень полиморфизма еще иногда называют «пермутацией» (от анг,- перестановка).

**45. Противодействие средствам обнаружения вторжений. Классификация методов. Методы на преобразования импорта исполняемых файлов.**

На этапе формирования загрузочного модуля компоновщик оснащает программу служебными заголовками и таблицами импорта и экспорта, содержащими информацию о требуемых программой внешних функциях. Затем загрузчик операционной системы, пользуясь этими заголовками и таблицами, обеспечивает программу необходимыми ресурсами - адресами внешних функций. Метод преобразования на основе модификации импорта, как раз и подразумевает видоизменение содержимого таких таблиц. Две составляющие; - наполнение тела программы фиктивными импортируемыми функциями; - удаление «подозрительных» импортируемых функций из тела программы. Задача наполнения тела программы фиктивными импортируемыми функциями заключается в заполнении его таблицы импорта функциями, которые нигде в коде не вызываются. Служит это для того, чтобы создавать видимость какого-то “безобидного” приложения. Существует несколько вариантов решений для такой задачи. Наиболее простой - это добавление к откомпилированому ассемблерному коду имен функций, с указанием количества параметров и директивой EXTERN Задача удаления «подозрительных» импортируемых функций из тела программы в свою очередь также может быть решена несколькими вариантами. Первый из них, это вызов соответствующих функций через связку «LoadLibrary - GetProcAddress». Результат вызова функций через эту связку, на примере программы выводящей «окно сообщений». Однако, стоит отметить, что такой вариант «маскировки» импортируемых функций может вызывать дополнительное детектирование. Второй вариант, заключается в обработке служебной структуры РЕВ/ТЕВ/TIB. Каждый процесс в Windows представлен блоком процесса, создаваемым исполнительной системой (EPROCESS). Кроме многочисленных атрибутов, относящихся к процессу, в блоке ЕРRОСЕSS содержатся указатели на некоторые структуры данных. Так, у каждого процесса есть один или более потоков, представляемых блоками потоков исполнительно" системы (ЕТН-ВЕАD). Блок EPROCESS и связанные с ним структуры данных - за исключением переменных окружения процесса (Process Environment Block, PEB) -- существующих в системном пространстве, Структура РЕВ находится в адресном пространстве процесса, так как содержит данные, модифицируемые кодом . пользовательского режима. Для каждого процесса, выполняющего Windows-программу, процесс подсистемы Windows поддерживает в дополнение к блоку EPROCESS параллельную структуру данных. Кроме того, часть подсистемы Windows, работающая в режиме ядра (Win32k.sys) поддерживает структуру данных для каждого процесса, которая создается при первом вызове потоком любой функции USER или GDI, реализованной в режиме ядра.

**46.Понятие информационной энтропии.**

Под понятием энтропия понимается мера эффективности хранения информации. Так же есть еще одно определение(подробное): Энтропия (информационная) — мера хаотичности информации, неопределённость появления какого-либо символа первичного алфавита. При отсутствии информационных потерь численно равна количеству информации на символ передаваемого сообщения. Для подсчета энтропии при реализации метода преобразования с использованием алгоритмов сжатия, применяется формула Клода Шеннона:  где N -- количество всех байтов в последовательности, b - единицы измерения (2 - биты, 3 - триты, и т.д.), Рi частота появления байта в последовательности. Энтропия ограничивает максимально возможное сжатие без потерь (равна минимальному количеству бит, которое необходимо для записи этого сообщения без искажений)