333333

**ЛЕКЦИЯ 14. Игра в прятки.**

**Сегодняшняя лекция, как и предыдущие, не совсем адекватна (точнее, совсем неадекватна). Далее представлен Глоссарий, «выдранный» из одной рекомендованной в рамках курса книги. Некоторые толкования слов вырезаны-спрятаны (некоторые по «принципу Веренича»). Некоторые вот так: D ytrjnjhs[ njkrjdfybz bpvtytytys ckjdf bkb gjcktljdfntkmyjcnm ckjd d chfdytybb c jhbubyfkjv. А некоторые так: . Ваша задача взять листочки (нормальные листочки, не обмылки, как обычно имеет место быть у jcj,j выдающихся особ), подписать их ХОРОШИМ ПОЧЕРКОМ, и далее по ходу чтения глоссария ВЫПИСЫВАТЬ НА ЛИСТОЧКИ ТОЛКОВАНИЯ (ПОЛНОСТЬЮ ПРАВИЛЬНЫЕ И НАПИСАННЫЕ ПЕЧАТНЫМИ БУКВАМИ!) Где их брать? ТОЛЬКО НЕ ИЗ ГОЛОВЫ СВОЕЙ! Искать! Только не в «… педиях»!**

**Лекция называется «Игра в прятки»! В конце текущей лекции листочки будут собраны (сколько успеете, чем больше, тем лучше, но лучше «меньше, да лучше». Хочется посмотреть, чем Вы занимаетесь на Лекции). В начале следующей лекции необходимо сдать работу над ошибками - текст, отпечатанный 12 шрифтом, со всеми толкованиями с указанием даты и времени завершения работы ПО КАЖДОМУ ПОНЯТИЮ!!!**

**Снова просьба. Не используйте чужой рабский труд и не будьте рабами и (или) рабовладельцами!!!**

**За каждое правильно расшифрованное (записанное) толкование получаете от 2 до 4 баллов, за неверно расшифрованное (записанное) толкование от минус 2 до минус 4-х (как и за отсутствие). За ЧРТыхание – двойной минус. Обращайте внимание на то, что по сравнению с глоссарием из книги некоторые термины изменены (убрана ненормативная лексика). Поэтому там, где дано полное толкование, нужно сравнивать то, что написано в данной лекции, с тем, что написано в книге, но использовать то, что написано в ЛЕКЦИИ 14!!!!**

**Глоссарий**

**(терминологический словарь)**

***Авторизация*** (authorization) — полномочия, устанавливаемые администратором системы для конкретных лиц, позволяющие последним использовать транзакции, процедуры или всю систему в целом.

***Администрирование средств безопасности*** включает в себя распространение данных, необходимых для работы сервисов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение криптографических ключей, установка прав доступа, анализ регистрационного журнала и т. п.

***Анализ затрат/выгоды*** (cost-benefit analysis) — стадия в разработке или развитии системы, на которой определяется *стоимость обеспечения защиты данных в информационной системе*; иногда под этой стоимостью подразумевают ущерб, который может быть нанесен в случае утери или компрометации данных, подлежащих защите.

***Атака*** (attack) — нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой. Это действие некоторого субъекта компьютерной системы (пользователя, программы, процесса и т. д.), использующего ее уязвимость для достижения целей, выходящих за пределы авторизации данного субъекта в данной компьютерной системе. Если, например, пользователь не имеет права на чтение некоторых данных, хранимых в компьютерной системе, а ему хочется незаконно его приобрести, он предпринимает ряд нестандартных манипуляций, либо обеспечивающих доступ к этим данным (в случае отсутствия или недостаточно надежной работы средств безопасности) либо завершившихся неудачей (в случае надежной работы средств безопасности). Тем самым этот пользователь (иногда его называют «захватчиком») предпринимает в отношении компьютерной системы атаку.

***Аутентификация*** (authentication) — 1) проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности; 2) план, разрабатываемый для обеспечения защиты от незаконных передач информации за счет установления санкционированных потоков информации, сообщений, узлов или инициаторов.

***Безопасность*** (security) — состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами. Безопасность обеспечивается путем создания вокруг компьютера и оборудования защищенной зоны, в которой работает только авторизованный персонал, а также использования специального программного обеспечения и встроенных в операционные процедуры механизмов защиты.

***Безопасность данных*** (data security) — защита данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашений.

***Безопасность информационной системы*** (information system security) — совокупность элементов (действий, мер), необходимых для обеспечения адекватной защиты компьютерной системы, включая аппаратные/программные функции, характеристики и средства; операционные и учетные процедуры, средства управления доступом на центральном компьютере, удаленных компьютерах и телекоммуникационных средствах; административные мероприятия, физические конструкции и устройства; управление персоналом и коммуникациями.

***Вирус*** (virus) — программа, модифицирующая другие программы. В контексте проблем безопасности этот термин обычно используется в отношении программ, злонамеренно внедряемых в систему с целью нанесения вреда или разрушений. Вирусная программа распространяется за счет самокопирования и подсоединения копий к другим программам. Когда в системе происходит определенное событие, на которое настроен вирус, вирус начинает выполнять свою целевую функцию. В настоящее время известны десятки тысяч программных вирусов, число которых непрерывно растет.

***Вирусы загрузочные*** внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).

***Вирусы файлово-загрузочные*** заражают как файлы, так и загрузочные секторы дисков.

***Вирусы файловые*** внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения .com и .ехе. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.

***Вирусы-мутанты*** содержат алгоритмы шифровки-дешифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

***Вирусы-невидимки — стелс-вирусы,*** которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

***Доступность*** (availability) — возможность получение информации авторизованным пользователем в нужное для него время.

***Защита информации*** (ЗИ) — процесс по предотвращению утечки защищаемой информации, санкционированных и непреднамеренных воздействий на защищаемую информацию, т. е. процесс, направленный на достижение состояния защищенности (тогда как информационная безопасность — это состояние защищенности информационной системы).

***Идентификация*** (identification) — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. Процесс анализа персональных, технических или организационных характеристик или кодов для получения (предоставления) доступа к компьютерным ресурсам.

***Информационная безопасность*** — состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование

***Компьютерная безопасность*** (computer security) — комплекс технологических и административных мер, применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

***Межсетевые экраны*** (FireWall) — устройство, программа, которые осуществляют фильтрацию данных на основе заранее заданной базы правил, что позволяет реализовывать гораздо более гибкую политику безопасности по сравнению с традиционными операционными системами. При комплексной фильтрации, охватывающей сетевой, транспортный и прикладной уровни, в правилах могут фигурировать сетевые адреса, количество переданных данных, операции прикладного уровня, параметры окружения (например, время) и т. п.

***Обнаружение***, ***основанное на сигнатурах***, — процесс обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с описаниями известных атак, составленному авторами программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в словаре, программа-антивирус может убить, удалить либо поместить в «райский уголок» зараженный файл.

***«Оранжевая» книга*** (orange book) — полное название «Department of Defence Trusted Computer System Evaluation Criteria» DOD 5200.28-STD («Критерии безопасности доверенных/надежных компьютерных систем министерства обороны США») — государственный стандарт оценивания безопасности компьютерных систем, устанавливающий четыре иерархических класса — А, В, С и D — определенных уровней доверенности (иными словами, уверенности в безопасности) для конкретных приложений, разрабатываемых и используемых в интересах правительства.

***Программы-детекторы*** позволяют обнаруживать программы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в программах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в какой-либо программе на экран выводится соответствующее сообщение.

***Резидентный вирус*** при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

***Сигнатура атаки*** (вируса) — характерные признаки атаки (вируса), используемые для их обнаружения. Это либо «синтаксические»

сигнатуры, взятые непосредственно из тела атаки (файла вируса и пр.), либо сигнатуры, ***основанные на аномалиях поведения программы, например, слишком активное обращение к какому-либо сетевому порту на компьютере.***

***СРД*** (система разграничения доступа — security policy realization) — совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

***Страница доступа к данным —*** опубликованная с помощью MS Access Web-страница, имеющая подключение к базе данных.

С помощью страниц доступа к данным можно просматривать, добавлять, изменять и обрабатывать данные, хранящиеся в базе данных. Страницы доступа к данным могут также содержать данные из других источников, таких как MS Excel [MSA].

***Субъект*** (subject) — активная сущность (процесс, пользователь, устройство и т. д.), вызывающая образование информационного потока между объектами или изменения состояния системы.

***Субъект доступа*** (access subject) — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

***Сценарий*** — именованный набор входных значений, которые можно подставить в электронную таблицу.

***Троянский конь*** (trojan horse) — компьютерная программа, имитирующая выполнение или реально выполняющая некоторую полезную функцию, но в то же время выполняющая и некоторую дополнительную (скрытую) функцию, позволяющую обойти систему защиты за счет скрытого использования законной авторизации вызывающего процесса. В ней содержится недокументированный (скрытый) модуль, который не вызывает подозрения и в дальнейшем выполняет недопустимые действия.

***Угроза*** (threat) — характеристики, свойства, условия системы и окружающей ее среды, которые в соответствующих условиях могут вызвать появление опасного события. Для компьютерной системы — это условия, представляющие потенциальную возможность нанесения ущерба компьютерной системе. Атаки — частный вид угроз так же, как и стихийные бедствия, человеческие ошибки, программные сбои и т. д.

***Управление доступом*** (access control) — в сетях или их компонентах — задачи, выполняемые аппаратурой, программным обеспечением и администрацией с целью отслеживания выполняемых в системе операций, целостности данных, доступа и модификаций системных записей, выполнения пользователями идентификации и предоставление пользователям доступа.

***Целостность*** (integrity) — состояние, в котором данные или программы спользуются установленным образом, обеспечивающим устойчивую работу системы; автоматическое восстановление в случае обнаружения системой потенциальной ошибки; автоматическое использование альтернативных компонентов вместо вышедших из строя. Примером является дублирование важных файлов с тем, чтобы в случае обнаружения ошибки или утери оригинального файла использовать его копию. Другим примером является поддержание двух и более путей доступа к устройству хранения.

***Целостность системы*** (system integrity) — состояние системы, в котором существует полная гарантия того, что при любых условиях компьютерная система базируется на логически завершенных аппаратных и программных средствах, обеспечивающих работу защитных механизмов, логическую корректность и достоверность операционной системы и целостность данных.

***Червь*** (worm) — программа, внедряемая в систему, часто злонамеренно, и прерывающая ход обработки информации в системе. Это программы, которые распространяются через сеть, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. В отличие от вирусов червь обычно не искажает файлы данных или программы. Обычно червь выполняется, оставаясь необнаруженным, и затем самоуничтожается.

***Эвристическое сканирование —*** метод работы антивирусной программы, основанный на сигнатурах и эвристике, призван улучшить способность сканеров применять сигнатуры и распознавать модифицированные версии вирусов в тех случаях, когда сигнатура совпадает с телом неизвестной программы не на 100 %, но в подозрительной программе налицо более общие признаки вируса. Данный подход, однако, может повысить количество ложных срабатываний.