**ЛЕКЦИЯ 16. Игра в прятки.**

**Сегодняшняя лекция, как и предыдущие, не совсем адекватна (это я себе льщу). Далее представлен Глоссарий, «выдранный» из одной рекомендованной в рамках курса книги. Некоторые толкования слов вырезаны-спрятаны. 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!!!) ТОЛЬКО ТЕХ СЛОВ и СЛОВОСОЧЕТАНИЙ, которые ОТСУТСТВУЮТ в тексте глоссария либо в толкованиях пропущены слова. Где их брать? ТОЛЬКО НЕ ИЗ ГОЛОВЫ СВОЕЙ!!!!! Искать!!!!!!! Лекция называется «Игра в прятки»!!!!! В конце лекции листочки будут собраны. Только просьба. Не используйте чужой рабский труд и не будьте рабовладельцем!!! Slave&slaveholder live matter!**

**Глоссарий**

**(терминологический словарь)**

***Автоконтроль целостности —*** использование в программе специальных алгоритмов, позволяющих после запуска программы определить, были ли внесены изменения в файл, из которого загружена программа, или нет.

***Авторизация*** (authorization) —

***Администрирование средств безопасности*** включает в себя распространение информации, необходимой 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.

***Анализ риска*** (risk analysis) — процесс изучения характеристик и слабых сторон системы, проводимый с использованием вероятностных расчетов, с целью определения ожидаемого ущерба в случае возникновения неблагоприятных событий. Задача анализа риска состоит в определении степени приемлемости того или иного риска в работе системы.

***Атака*** (attack) —

***Аудит*** (audit) — контроль, образ действий, позволяющий получать независимый обзор и анализ системных записей об активности

системы с целью установления ее текущего состояния безопасности.

***Аутентификация*** (authentication) —

***Безопасность*** (security) — состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал \*

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

***Безопасность информации*** (information security) — состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

***Безопасность информационной системы*** (information system security) —

***Безопасность коммуникаций*** (communications security) — аутентификация телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам критичной информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

***Брешь***, ***дыра*** (loophole) — программное или аппаратное упущение или недоработка, позволяющая обойти процессы управления

доступом. Синонимы — fault, flaw.

***Вирус*** (virus) — 



***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 и **.** 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) —

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

***Защита персональной информации*** (privacy protection) — совокупность технических, административных и физических мер, реализованных с целью обеспечения безопасности и конфиденциальности записей данных, равно как и для защиты подсистем безопасности и конфиденциальности от любых случайных или преднамеренных действий, которые могут привести к затруднению, ущербу, неудобствам или несправедливости в отношении

лица, о котором хранится соответствующая информация.

***Идентификация*** (identification) —

***Информационная безопасность*** —

***Компрометация*** (compromise) — утеря критичной информации либо получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т. д.).

***Компьютерная безопасность*** (computer security) —

***Конфиденциальная информация*** (sensitive information) — информация, требующая защиты, а именно: критичная информация с различными грифами секретности; информация для служебного пользования; информация, составляющая коммерческую тайну или тайну фирмы; информация, являющаяся собственностью некоторой организации или частного лица и т. д.

***Конфиденциальность*** (confidentiality) — доступность информации только определенному кругу лиц, данных, получение либо использование которых неавторизованными для этого лицами может стать причиной серьезного

ущерба для организации.

***Люк*** (trap door) — скрытый программный или аппаратный механизм, позволяющий обойти механизмы защиты системы. Обычно это использование недокументированных точек входа (они вставляются в программы на стадиях разработки или наладки, а затем при определенных условиях оказываются лишними и неудаленными) для проникновения в систему. Существует два основных типа люков: внутренние и внешние. К первым относятся некоторые внутренние элементы системы (например, дата-временное значение, счетчик и т. д.), определяющие требуемые условия; к другому типу относятся внешние элементы (например, удаленный терминал).

***Межсетевой экран*** (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.

***Многоуровневая защита*** (multilevel secure) — защита, обеспечивающая разграничение доступа субъектов с различными правами

доступа к объектам различных уровней конфиденциальности.

***Модификация —*** осуществление третьей неавторизованной стороной не только доступа к компоненту, но и манипуляций с ним. Например, модификациями являются неавторизованное изменение данных в базах данных или вообще в файлах компьютерной системы, изменение алгоритмов используемых программ с целью выполнения некоторой дополнительной незаконной обработки. Иногда модификации обнаруживаются достаточно быстро (если не сразу), но более тонкие модификации могут оставаться необнаруженными весьма длительное время.

***НСД*** (несанкционированный доступ к информации — unauthorized access to information) — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств (совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем).

***Обнаружение***, ***основанное на сигнатурах***, — метод работы антивирусов и систем 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 удалить, «вылечить» либо поместить в «карантин» 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») — госу­

дарственный 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.

***Пароль*** (password) — идентификатор субъекта доступа, который является его (субъекта) секретом.

***Персональный идентификационный номер*** (Personal Identification

Number — PIN) — персональный код некоторого лица, обеспечивающий ему возможность входа в систему с управляемым

доступом.

***Программы-детекторы*** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем

диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.

***Резервное копирование*** (backup) — процесс создания копии данных на внешнем носителе, что позволяет осуществлять быстрое и недорогое восстановление информации (документов, программ, настроек и т. д.) в случае утери рабочей копии информации по какой-либо причине. Кроме этого решаются смежные проблемы — дублирование данных, передача данных и работа с общими документами и т. д.

***Резидентный вирус***

***Санкционированный доступ к информации*** (authorized access to information) — доступ к информации, не нарушающий правила

разграничения доступа.

***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 [MSAJ.

***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.

— именованный набор входных значений, которые можно подставить в электронную т.

.

***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 по­

дозрения 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.

***Уязвимость*** (vulnerability) — любая ошибка или слабая проработка (например, неопределенность условий обработки), существующая в системе. Уязвимость создает предпосылки для нарушения безопасности системы. При этом уязвимость существует независимо от того, известны какие-либо угрозы или нет. Уязвимость может существовать либо только теоретически, либо иметь известный эксплойт.

***Физическая безопасность*** (physical security) — совокупность охраны, замков, пропусков и других средств управления физическим доступом к компьютеру и периферии. Термин употребляется также в отношении средств защиты помещений, в которых находится оборудование, от пожара, стихийных бедствий и катастроф.

***Физическая целостность информации —*** отсутствие искажений или уничтожения элементов информации.

***Целостность*** (integrity) — состояние, в котором данные или программы используются 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 данных*** (data integrity) — состояние, при котором данные, представленные в компьютере, в точности соответствуют

данным в исходных документах и при этом не могут быть подвержены неумышленным или умышленным искажениям или

разрушениям.

***Целостность информации*** (information integrity) — способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

***Целостность системы*** (system integrity) —

***Цифровая подпись*** — шифрованная электронная подпись, подтверждающая подлинность макроса или документа. Наличие цифровой подписи подтверждает, что макрос или документ был получен от владельца подписи и не был изменен [MSOF].

***Цифровой сертификат*** — вложение в файл, проект макроса или сообщение электронной почты, подтверждающее его подлинность, обеспечивающее шифрование или предоставляющее поддающуюся проверке подпись. Для цифрового подписывания проектов макросов необходимо установить цифровой сер­

тификат [MSOF].

***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. Данная технология, однако, может повысить количество ложных срабатываний.

***Электронная цифровая подпись*** (ЭЦП) — реквизит электронного документа, предназначенный для защиты данного электронного

документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.