2. Основы защиты информации

Информационная безопасность

В Доктрине информационной безопасности Российской Федерации понятие «информационная безопасность» трактуется в широком смысле.

Оно определяется как состояние защищенности национальных интересов в информационной сфере при сбалансированности интересов личности, общества и государства.

Под информационной безопасностью принято понимать способность информации сохранять неизменность своих свойств при воздействии случайных или преднамеренных внешних воздействий. К числу свойств, обеспечивающих безопасность информации, относятся:

• доступность информации — способность обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации;

• целостность информации — способность существовать в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Это свойство включает физическую целостность данных, их логическую структуру и содержание;

• конфиденциальность информации — способность системы (среды) сохранять информацию в тайне от субъектов, не имеющих полномочий на доступ к ней.

Информационная безопасность автоматизированной системы — это состояние автоматизированной системы, при котором она, с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — затраты на ее функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации.

Программно-технические методы защиты информации включают:

- идентификацию и аутентификацию,

- управление доступом,

- протоколирование и аудит,

- экранирование,

- шифрование,

- антивирусную защиту.

Современные информационные системы требуют использования схемы безопасности с обязательным или принудительным контролем доступа к данным, основанном на «метках безопасности».

Каждая метка соответствует конкретному уровню.

Использование меток позволяет классифицировать данные по уровням безопасности.

Для правительственных информационных систем такая классификация выглядит следующим образом:

- совершенно секретно;
- секретно;
- конфиденциальная информация;
- неклассифицированная информация.

Разработке необходимых защитных мер для конкретного информационного объекта всегда должен предшествовать анализ возможных угроз: их идентификация, оценка вероятности появления, размер потенциального ущерба.

Наиболее распространенными угрозами считаются:

- сбои и отказы оборудования;
- ошибки эксплуатации;
- программные вирусы;
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, хакеров, диверсантов и т.п.);
- стихийные бедствия и аварии.

Идентификация и аутентификация

Идентификация позволяет субъекту (пользователю или процессу, действующему от имени пользователя) назвать себя (сообщить свое имя).

Посредством ***аутентификации*** вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает.

В качестве синонима слова «аутентификация» иногда используют словосочетание «проверка подлинности».

Если в процессе аутентификации подлинность субъекта установлена, то система защиты определяет для него полномочия доступа к информационным ресурсам.

Большинство экспертов по безопасности считают, что обычные статические пароли не являются надежным средством безопасности, даже при соблюдении строгих правил их использования.

Наблюдение за действиями пользователя при работе с компьютером может раскрыть пароль.

Для решения этой проблемы используются одноразовые пароли, которые выдаются специальными устройствами (***токенами***).

Подделка пароля и неавторизованный вход в систему становятся крайне трудновыполнимыми задачами.

Токены способны осуществлять проверку пин-кода и подтверждение введенных данных самостоятельно, не требуя физического подключения к компьютеру и не имея в момент фактического проведения авторизации логического соединения с защищаемой системой.

Управление доступом

Программные средства управления доступом позволяют специфицировать и контролировать действия, которые пользователи или процессы в соответствии с полномочиями, назначенными им системой защиты, могут выполнять над информацией и другими ресурсами системы.

Это основной механизм обеспечения целостности и конфиденциальности объектов в многопользовательских информационных системах.

Имеется несколько уровней доступа к информационному объекту:

- редактирование (удаление, добавление, изменение);
- просмотр (чтение);
- запрет доступа.

Протоколирование и сетевой аудит

Протоколирование — это сбор и накопление информации о событиях, происходящих в информационной системе в процессе ее функционирования.

Аудит — это анализ накопленной информации, проводимый оперативно или периодически (например, один раз в день).

Реализация протоколирования и аудита в системах защиты преследует следующие основные цели:

- обеспечение подотчетности пользователей и администраторов;

- обеспечение возможности реконструкции последовательности событий;

- обнаружение попыток нарушения информационной безопасности;

- предоставление информации для выявления анализа проблем.

Принцип работы ***систем обнаружения нарушения информационной безопасности*** заключается в том, что отслеживаются аномалии сетевого трафика.

Отклонения в большинстве случаев являются признаком сетевой атаки.

Например, нетипичная длина сетевого пакета, неполная процедура установления соединения — все эти критерии фиксируются системами обнаружения атак (СОВ).

У данного способа обнаружения атак был и остается один существенный недостаток — он имеет дело с уже свершившимися событиями, т.е. с уже реализованными атаками.

Знания о совершенных несанкционированных действиях позволяют предотвратить повторение этих действий.

Экранирование

Экран контролирует информационные потоки между узлами сети.

Контроль потоков состоит в их фильтрации с выполнением некоторых преобразований.

Фильтрация информационных потоков осуществляется ***межсетевыми экранами*** на основе ***набора правил,*** определяемых политикой безопасности организации.

Межсетевые экраны производят логический анализ получаемой информации.

При этом учитываются содержание информации, порт, через который поступил сетевой запрос, и т.д.

Шифрование

Различают два основных метода шифрования: симметричный и асимметричный.

В первом из них один и тот же ключ (хранящийся в секрете) используется и для шифрования, и для расшифровки данных.

Во втором используются два ключа.

Один из них, несекретный (он может публиковаться вместе с адресом пользователя), используется для шифрования сообщения, другой, секретный (известный только получателю) — для расшифровки.

Криптография необходима для реализации трех сервисов безопасности: шифрования; контроля целостности и аутентификации .

Электронная подпись

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, предназначенный для зашиты 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.

Алгоритм шифрования подписи должен определять ***секретный ключ пользователя***, известный только владельцу ключа.

Алгоритм проверки правильности подписи должен определять ***открытый ключ пользователя***, известный абонентам-получателям.

При таком подходе воспользоваться подписью может только владелец ключа, а проверить ее подлинность — любой абонент, которому передан открытый ключ, путем дешифрования сообщения этим ключом.

Антивирусная защита

Классификация вирусов. ***Компьютерный вирус*** — это программа, способная к самостоятельному размножению и функционированию, и имеющая защитные механизмы от обнаружения и уничтожения. В настоящее время известно более 5000 программных вирусов, которые можно классифицировать по различным признакам.

В зависимости от среды обитания вирусы подразделяются на сетевые, файловые и загрузочные.

Сетевые вирусы распространяются по различным компьютерным сетям.

Файловые вирусы инфицируют главным образом исполняемые файлы с расширениями COM и EXE.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска.

По способу заражения вирусы делятся на резидентные и нерезидентные.

Резидентные вирусы при заражении компьютера помещаются в оперативную память. Они перехватывают обращения операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.п.) и внедряются в них.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия, можно лишь выделить основные типы:

- ***простейшие вирусы*** (***вирусы-паразиты***) изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены;
- ***вирусы-репликаторы*** (***черви***) распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. Вирусы-черви не изменяют содержимое файлов, однако они очень опасны, так как уменьшают пропускную способность сети и замедляют работу серверов;
- ***вирусы-невидимки*** (***стелс-вирусы***) очень трудно обнаруживаются и обезвреживаются, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска;

• вирусы-мутанты содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов;

• квазивирусные, или «троянские», программы не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков или собирают на компьютере информацию, не подлежащую разглашению.

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с носителя информации, содержащего вирус.

Основные признаки появления вирусов:

• медленная работа компьютера, частые зависания и сбои;

• исчезновение файлов и каталогов или искажение их содержимого;

• изменение размера, даты и времени модификации файлов;

• значительное увеличение количества файлов на диске;

• уменьшение размера свободной оперативной памяти;

• вывод на экран непредусмотренных сообщений или звуковых сигналов.

Классификация антивирусных программ. Антивирусные программы подразделяются на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Программы- детекторы позволяют обнаруживать файлы, зараженные одним из известных вирусов. Эти программы проверяют файлы на указанном пользователем логическом диске на наличие в них специфической для данного вируса комбинации байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Большинство программ-детектров имеют режимы лечения или уничтожения зараженных файлов. Программы-детекторы, как правило, не способны обнаруживать в памяти компьютера «невидимые» вирусы.

Программы-ревизоры запоминают сведения о состоянии системы (до заражения), после чего на всех последующих этапах работы программа-ревизор сравнивает характеристики программ и системных областей дисков с исходным состоянием и сообщает пользователю о выявленных несоответствиях. Как правило, сравнение состояний производится сразу после загрузки операционной системы. При сравнении проверяются длина файла, контрольная сумма файла, дата и время последней модификации. Многие программы-ревизоры могут отличать изменения в файлах, сделанные пользователем, от изменений, вносимых вирусом, так как вирусы обычно производят одинаковые изменения в разных программных файлах.

Программы-доктора, или фаги — программы, которые не только обнаруживают зараженные файлы и системные области дисков, но и «лечат» их в случае заражения. Вначале своей работы фаги ищут вирусы в оперативной памяти, уничтожают их, после чего переходят к «лечению» файлов. Среди фагов можно выделить ***полифаги***, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Программы-фильтры, или «сторожа» располагаются в оперативной памяти компьютера и перехватывают обращения к операционной системе, которые могут использоваться вирусами для размножения и нанесения вреда программной среде:

- попытки коррекции загрузочных файлов;
- изменение атрибутов файлов;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия, «сторож» сообщает об этом пользователю и предлагает разрешить или запретить выполнение соответствующей операции. Программы-фильтры позволяют обнаружить вирус в программной среде на самых ранних этапах его существования, еще до размножения.

Программы-вакцины (или иммунизаторы) — резидентные программы, предотвращающие заражение файлов. Вакцины модифицируют программные файлы и диски таким образом, что это не отражается на их работе, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными и поэтому в них не внедряется.

Антивирусные программы. Наиболее популярными в России антивирусными программами являются ***ADinf, Dr Web, Aidtest, Norton Antivirus, Symantec Antivirus, Антивирус Касперского*** (***AVP***).

Norton Antivirus — одна из самых известных в мире антивирусных программ — производится американской компанией Symantec. Программа неоднократно занимала призовые места в крупнейших международных антивирусных тестах. Для корпоративных сетей компанией выпускается специальная версия ***Symantec Anti Virus***.

К числу программ-ревизоров файловых систем относится широко распространенная в России программа ***Adinf*** фирмы «Диалог-Наука».

Aidstest— антивирусная программа — сканер (полифаг). Автор Д.М. Лодзинский. Версии Aidstest регулярно обновляются и пополняются информацией о новых вирусах.

Программа-полифаг ***Doctor Web*** (Россия) предназначена прежде всего для борьбы с полиморфными вирусами, вирусами-мутантами. Программа может определять файлы, зараженные новыми, неизвестными вирусами, проникая в зашифрованные и упакованные файлы. Это достигается благодаря наличию достаточно мощного эвристического анализатора.

Одним из наиболее распространенных антивирусных средств является система *AVP* (***AntiViral Toolkit Pro***), созданная в России «Лабораторией Касперского». Система имеет одну из самых больших вирусных баз данных. Постоянное пополнение этой базы позволяет системе обнаруживать практически все полиморфные вирусы, предоставляет пользователю защиту от троянских и шпионских программ.

К основным недостаткам антивирусных средств следует отнести необходимость постоянного обновления вирусных баз.