Средства безопасности сетевых ОС

Защита сетевых операционных систем

Операционная система и аппаратных средства сети обеспечивают защиту ресурсов сети, одним из которых является сама ОС, т.е. входящие в нее программы и системная информация. Поэтому в сетевой ОС ЛВС должны быть так или иначе реализованы механизмы безопасности.

Принято различать:

- пассивные объекты защиты (файлы, прикладные программы, терминалы, области оперативной памяти и т.п.);
- активные субъекты (процессы), которые могут выполнять над объектами определенные операции.

Защита объектов реализуется операционной системой посредством контроля за выполнением субъектами совокупности правил, регламентирующих указанные операции. Указанную совокупность иногда называют ***статусом защиты***. Операции, которые могут выполняться над защищенными объектами, принято называть ***правами доступа***, а права доступа субъекта по отношению к конкретному объекту — ***возможностями***. В качестве ***формальной модели статуса защиты*** в ОС чаще всего используется так называемая ***матрица контроля доступа***.

Достаточно простым в реализации средством разграничения доступа к защищаемым объектам является ***механизм колец безопасности***.

Защита файлов в ОС организована следующим образом:

С каждым файлом связывается множество прав доступа: чтение, обновление и (или) выполнение (для исполняемых файлов). Владелец файла, т.е. создавшее его лицо, пользуется но отношению к файлу всеми правами. Часть этих прав он может передать членам группы.

- выбор и установка средств защиты;
- обследование информационной системы (ИС) на предмет установления ее организационной и информационной структуры и угроз безопасности информации;
- подготовка персонала работе со средствами защиты;
- организация обслуживания по вопросам информационной безопасности;
- создание системы периодического контроля информационной безопасности ИС.

В результате изучения структуры ИС и технологии обработки данных в ней разрабатывается **Концепция информационной безопасности** ИС, на основе которых в дальнейшем проводятся все работы по защите информации в ИС. В концепции находят отражение следующие основные моменты:

- организация сети организации;
- существующие угрозы безопасности информации, возможности их реализации и предполагаемый ущерб от этой реализации;
- организация хранения информации в ИС;
- организация обработки информации; (на каких рабочих местах и с помощью какого программного обеспечения);
- регламентация допуска персонала к той или иной информации;

- ответственность персонала за обеспечение безопасности.

В конечном итоге на основе Концепции информационной безопасности ИС создается **схема безопасности,** структура которой должна удовлетворять следующим условиям.

- 1. Защита от несанкционированного проникновения в корпоративную сеть и возможности утечки информации по каналам связи.
- 2. Разграничение потоков информации между сегментами сети.
- 3. Защита критичных ресурсов сети.
- 4. Защита рабочих мест и ресурсов от несанкционированного доступа (НСД).
- 5. Криптографическая защита информационных ресурсов.

В настоящее время не существует однозначного решения, аппаратного или программного, обеспечивающего выполнение одновременно всех перечисленных условий. Требования конкретного пользователя по защите информации в ИС существенно разнятся, поэтому каждая задача решается часто индивидуально с помощью тех или иных известных средств защиты. Считается нормальным, когда 10—15% стоимости информации тратится на продукты, обеспечивающие безопасность функционирования сетевой информационной системы.

Защиты операционных систем Windows

Развитие технологий привело к повсеместному использованию Интернета и облачных сервисов в организациях всё более широкому применению личных устройств сотрудников на рабочих местах в корпоративной сети и, как следствие, необходимости в удалённом доступе к рабочим ресурсам. Очевидно, что такие тенденции рынка способствуют ужесточению требований к информационной безопасности. Компания Microsoft предлагает своё видение вопросов безопасности, конфиденциальности и надёжности. Особое внимание при создании новой операционной системы для домашних и бизнес-пользователей Windows было уделено технологиям защиты данных. Новая система надёжно защищена, а улучшенные технологии обеспечивают как безопасность пользователей, так и всей ИТ-инфраструктуры компании, что создаёт надёжный фундамент для успешного развития бизнеса.

Безопасная загрузка SecureBoot. В Windows реализована функция безопасной загрузки SecureBoot на основе UEFI, которая позволяет защитить устройство в процессе загрузки системы. Что является весьма важным условием обеспечения безопасности, так как ряд вредоносных программ может попытаться закрепиться в операционной системе, подменяя собой её загрузочные записи. Функция SecureBoot в Windows предотвращает запуск кода без валидной цифровой подписи. В случае если вредоносная программа все-таки сможет вмешаться в процесс запуска, Windows автоматически это обнаружит и выполнит откат действий.

Антивирус Defender. В новую операционную систему также встроена усовершенствованная антивирусная программа Defender. Теперь пользователю не нужно устанавливать сторонние антивирусы для защиты компьютера. Defender запускается автоматически с началом работы системы. Кроме того, в новой Windows улучшено быстродействие антивирусной программы, которая к тому же ежедневно получает обновления.

Расширенные возможности идентификации и система хранения паролей. С появлением Windows 8 стала доступна ещё одна система защиты. Теперь у пользователя есть выбор варианта выполнения паролей для входа в систему - это PIN-код из четырёх цифр и «графический пароль». Выбрав последний вариант, пользователь сможет использовать в качестве пароля изображение или фотографию и создать определённую последовательность

прикосновений к ней. Например, можно обвести лицо на снимке, провести линию или придумать собственный объект для разблокировки. Данная функция позволяет предотвратить несанкционированный доступ к системе.

Кроме того, современные операционныеисистемы позволяет создавать виртуальные смарт-карты, функционирующие на основе доверенного модуля TPM (Trusted Platform Module). Таким образом, если пользователь боится потерять физическую карту, он может пользоваться виртуальной, безопасно хранящейся в TPM. Удалённые пользователи также могут работать с виртуальными смарт-картами, используя технологию Direct Access для безопасного подключения к корпоративной сети.

Со встроенной в Windows системой централизованного хранения паролей Credential Manager пользователям больше не нужно запоминать пароли для доступа к своим аккаунтам -вход в систему осуществляется с помощью единого аккаунта Microsoft. Учётные данные пользователя перед отправкой на серверы Microsoft шифруются и синхронизируются на всех компьютерах, помеченных как «доверенные».

Разграничение прав пользователей и приложений. Доступ пользователей к приложениям и работа с ними контролируются с помощью компонента AppLocker, позволяющего ИТ-администраторам обеспечивать безопасность с помощью групповой политики и тем самым предотвращать запуск потенциально опасных приложений. Кроме того, все приложения работают изолированно друг от друга: у каждого отдельная область, не ограничивающая его функционирование, но изолирующая от других приложений и ядра. При атаке вируса активного приложения другим программам и операционной системе ничего не угрожает. Прежде чем приложение разработчика появится в Магазине Windows, оно должно пройти проверку и сертификацию Microsoft, что даёт определённую гарантию пользователям того, что все приложения, представленные в Store, безопасны.

Важным аспектом обеспечения безопасности является возможность управления доступом к данным с целью их защиты от несанкционированного использования в случае кражи или потери. Данные, хранящиеся на локальных устройствах, позволяет защитить технология BitLocker, а содержащиеся на съёмных носителях - BitLocker To Go. В Windows существенно увеличилась скорость шифрования данных с помощью BitLocker. Усовершенствованная технология шифрует не весь диск целиком, а только занятое на нём пространство, что обеспечивает безопасность без ощутимого вмешательства в работу пользователей. Для разблокировки диска с зашифрованными данными потребуется пароль, Pin-код или смарт-карта.

Репутационный фильтр SmartScreen. Поднимая вопрос об обеспечении безопасности, которому уделено достаточно большое внимание в Windows, стоит также отметить встроенный фильтр SmartScreen. Он осуществляет проверку репутаций файлов и программ и, таким образом, обнаруживает и блокирует неизвестные и потенциально опасные файлы, приложения и архивы на USB-носителе, жёстком диске или загружаемые из Интернета, а также отражает атаки фишинговых сайтов. При первом запуске загруженной программы SmartScreen проверяет список известных безопасных приложений и в случае опасности выдаёт предупреждение. Фильтр работает с любым используемым браузером.

Так, технология Address Space Layout Randomization (ASLR) предотвращает создание корректно и стабильно работающих эксплоитов, которые основываются на знание размещения DLL в ОЗУ.

Обновлённая ASLR распространяется на большее количество внутренних структур операционной системы, отражая атаки, направленные на обход технологии в её прежних версиях.

Функция восстановления заводских настроек. В случае возникновения необходимости сбросить настройки компьютера, пользователь может воспользоваться расширенной опцией удаления всех данных и переустановки Windows, которая восстановит заводские настройки. Все данные и установленные программы будут удалены. В системе хранятся все резервные файлы, и функция «Восстановление ПК» позволяет пользователю, в случае обнаружения каких-то неполадок, совершить возврат к определённому моменту в прошлом, при этом сохранив данные программ.

Windows To Go для тех, кто ведёт мобильный образ жизни и при этом желает, чтобы Windows с привычными приложениями всегда был под рукой, появился Windows to go. По сути Windows to go - это USB-диск с ОС и приложениями. Загрузившись с него, вы получаете доверенную и привычную среду на любом оборудовании, поддерживающем Windows, и которое оказалось у вас под рукой.

Компания Microsoft предоставляет возможности корпоративных социальных коммуникаций, гарантируя безопасность и конфиденциальность, которые так необходимы бизнесу. Множество различных решений, которые предлагает современная операционная система Windows , обеспечивают надёжную защиту информации и устройств пользователей. Платформа Windows сочетает в себе не только удобство использования для сотрудников организаций, повышая тем самым общую производительность и эффективность труда, но и значительно упрощает работу ИТ-отдела по обеспечению безопасной среды внутри компании.

Проблема безопасности

Безопасность (security) – это защита от внешних атак. В настоящее время наблюдается значительный рост числа самых разнообразных атак хакеров, угрожающих целостности информации, работоспособности компьютерных систем и зависящих от них компаний, благосостоянию и личной безопасности людей. Для защиты от атак необходимы специальные меры безопасности, компьютерные технологии и инструменты.

В любой компьютерной системе должна быть реализована подсистема безопасности, которая должна проверять внешнее окружение системы и защищать ее от:

Несанкционированного доступа

Злонамеренной модификации или разрушения

Случайного ввода неверной информации.

Практика показывает, что легче защитить от случайной, чем от злонамеренной порчи информации.

Аутентификация

Одной из наиболее широко используемых мер безопасности является аутентификация (authentication) – идентификация пользователей при входе в систему. Такая идентификация пользователей наиболее часто реализуется через логины – зарегистрированные имена пользователей для входа в систему – и пароли – секретные кодовые слова, ассоциируемые с каждым логином.

Основной принцип использования паролей в том, что они должны сохраняться в секрете. Поэтому одна из традиционных целей атакующих хакеров состоит в том, чтобы любыми способами выведать у пользователя его логин и пароль. Для сохранения секретности паролей предпринимаются следующие меры.

Частая смена паролей. Аналогичные меры применялись в армии во время войны. Большинство сайтов и других систем (например, сайт партнеров фирмы Microsoft) требуют от пользователей регулярной (например, не реже. чем раз в три месяца) смены паролей, иначе сайт блокируется для доступа. Подобные меры вполне оправданы.

Использование "не угадываемых" паролей. Практически все системы требуют от пользователя при регистрации устанавливать пароли, не являющиеся легко угадываемыми: например, как правило, пароль должен содержать большие и маленькие буквы и цифры, специальные символы и иметь длину не менее 7-8 символов. Используются также автоматические генераторы не угадываемых паролей. Поэтому использование в качестве паролей легко угадываемых слов – например, имени любимой собаки или общеупотребительного понятия – не рекомендуется.

Сохранение всех неверных попыток доступа. Во многих системах реализован системный журнал, в котором фиксируются все неверные попытки ввода логинов и паролей. Обычно дается фиксированное число таких попыток (например, три).

Пароли также могут быть закриптованы или разрешены для доступа лишь один раз, после чего от пользователя требуется смена пароля.

Программные угрозы (атаки)

Рассмотрим некоторые типичные виды угроз и атак, используемые хакерами.

Троянская программа (Trojan Horse) – атакующая программа, которая "подделывается" под некоторую полезную программу, но при своем запуске не по назначению (злонамеренно) использует свое окружение, например, получает и использует конфиденциальную информацию. Троянские программы используют системные механизмы для того, чтобы программы, написанные одними пользователями, могли исполняться другими пользователями.

Вход в ловушку (Trap Door) - использование логина или пароля, который позволяет избежать проверок, связанных с безопасностью.

Переполнение стека и буфера (Stack and Buffer Overflow) - использование ошибки в программе (переполнение стека или буферов в памяти) для обращения к памяти другого пользователя или процесса с целью нарушения ее целостности.

Системные угрозы (атаки) - некоторые типичные атаки, использующие уязвимости (vulnerabilities) в системных программах – ошибки и недочеты, дающие возможность организации атак.

Черви (Worms) – злонамеренные программы, использующие механизмы самовоспроизведения (размножения). Например, один из Интернет-червей использует сетевые возможности UNIX (удаленный доступ) и ошибки в программах finger и sendmail. Принцип его действия следующий: некоторая постоянно используемая в сети системная программа распространяет главную программу червя.

вирусы – фрагменты кода, встраивающиеся в обычные программы с целью нарушения работоспособности этих программ и всей компьютерной системы. В основном вирусы действуют на микрокомпьютерные системы. Вирусы скачиваются с публично доступных

сайтов или с дисков, содержащих "инфекцию". Для предотвращения заражения *компьютерными вирусами* необходимо соблюдать принципы безопасности при использовании компьютеров (**safe computing**) – использовать **антивирусы**, **guards** – программы, постоянно находящиеся в памяти и проверяющие на вирусы каждый открываемый *файл* - .exe, doc, и т.д.

Отказ в обслуживании (Denial of Service – DoS) – одна из распространенных разновидностей атак на *сервер*, заключающаяся в создании искусственной перегрузки сервера с целью препятствовать его нормальной работе. Например, для Web-сервера такая *атака* может заключаться в том, чтобы искусственно сгенерировать миллион запросов "*GET*". Если *сервер* реализован не вполне надежно, подобная *атака* чаще всего приводит к переполнению памяти на сервере и необходимости его перезапуска.

Типы сетевых атак

Рассмотрим некоторые типы современных *сетевых атак*, которых необходимо постоянно остерегаться пользователям.

Phishing – попытка украсть *конфиденциальную информацию* пользователя путем ее обманного получения от самого пользователя. Даже само *слово* **phishing** – искаженное *слово* **fishing** (рыбная ловля), т.е. *хакер* с помощью этого приема как бы пытается поймать чересчур наивного пользователя "на удочку". Например, напугав в своем сообщении пользователя, что его логин и *пароль*, кредитная карта или банковский счет под угрозой, *хакер* пытается добиться от пользователя в ответ ввода и отправки некоторой *конфиденциальной информации*. Обычно *phishing*-сообщение *по* электронной почте приходит как бы от имени банка и подделывается под цвета, логотипы и т.д., используемые на сайте банка. Однако для его разоблачения обычно достаточно подвести *курсор* мыши (не *кликая* ее) к приведенной web-ссылке или *email*-адресу (при этом она высвечивается) и убедиться в том, что *адрес* указывает отнюдь не на банк, а на совершенно посторонний *сайт* или *email*. Поэтому пользователям не следует быть слишком наивными. Другая действенная *мера*, если *phishing* происходит регулярно с одних и тех же *email*-адресов, - включить эти адреса в черный *список* на *email*-сервере. Тогда подобные сообщения вообще не будут доходить до входного почтового ящика пользователя.

Pharming – перенаправление пользователя на злонамеренный Web-*сайт* (обычно с целью *phishing*). Меры предотвращения со стороны пользователя мы уже рассмотрели. В современные web-браузеры встроены программы антифишингового контроля, которые запускаются автоматически при обращении к сайту. Хотя это отнимает у пользователя некоторое время, подобные меры помогают предотвратить многие атаки.

Tampering with data – злонамеренное искажение или порча данных. Действенной мерой *по* борьбе с подобными атаками является **криптование** информации.

Spoofing – " подделка" под определенного пользователя (злонамеренное применение его логина, пароля и полномочий). Логин и *пароль* при этом либо получены от пользователя обманным путем (например, в результате *phishing*), либо извлечены из "взломанного" хакерской программой системного файла.

Elevation of privilege – попытка расширить полномочия (например, до полномочий системного администратора) с целью злонамеренных действий. Поэтому наиболее секретная *информация* в любой компьютерной системе – *пароль* системного администратора, который необходимо защищать особенно тщательно.

Trustworthy Computing (TWC) Initiative

Инициатива под таким названием (инициатива надежных и безопасных вычислений) объявлена в 2002 г. в историческом электронном письме основоположника корпорации Microsoft Билла Гейтса всем сотрудникам компании. Основная суть инициативы TWC заключается в том, что безопасности необходимо уделять особое внимание при разработке программной системы, начиная с самых ранних этапов. Однако этим инициатива TWC не исчерпывается – смысл и цели ее гораздо шире и охватывают также экономические, юридические аспекты и "*человеческий фактор*".

Основные принципы инициативы TWC:

Безопасность (Security) – реализация и использование в любой программной системе действенных мер защиты от внешних атак; использование специальных методов разработки программ, направленных на достижение этой цели.

Сохранение конфиденциальности информации (Privacy) – использование программным обеспечением частной и корпоративной информации только с явного согласия пользователя и только для понятных ему законных целей; защита *конфиденциальной информации* от взлома в результате атаки.

Надежность (Reliability) – *предсказуемость* поведения программных систем, которые должны обеспечивать в заданном окружении ожидаемое правильное поведение программы.

Оперативность, законность и корректность бизнеса (Business Integrity) – оперативность работы группы сопровождения программного продукта и своевременные консультации пользователей *по* вопросам безопасности; *корректность* бизнеса компании – разработчика программного обеспечения.

Сама *корпорация* Microsoft с 2002 г. полностью реорганизовала *бизнес-процессы разработки программного обеспечения*, используя новую схему жизненного *цикла* для разработки безопасных программ – **SDLC (Security Development Life Cycle)**.Принципы TWC воплощены во всех новых версиях продуктов Microsoft: *Internet* Explorer 7 и 8, *Windows Vista* и др.

Microsoft своей инициативой TWC призвала все остальные компании и индивидуальных разработчиков следовать предложенным ею принципам, хотя изначально *отношение* к инициативе TWC в мире было достаточно осторожным и даже скептическим.

Microsoft финансировала работы *по* обеспечению TWC и обучение TWC в университетах.

Следует отметить, что обучение TWC в университетах в мире только начато. Наибольшее внимание этим вопросам в первую *очередь* уделяют университеты военного подчинения и назначения.

Одним из первых университетов, обучающих студентов ИТ-*специальностей принципам* TWC, является математико-механический факультет СПбГУ – более подробное изучение TWC в курсе проф. В.О. Сафонова "Архитектуры и *модели программ* и знаний" (4 курс) и изложение элементов TWC во всех других курсах проф. В.О. Сафонова: "Операционные системы и сети", "Java-технология", "Компиляторы".

Принципы разработки безопасных программных продуктов

Новая схема жизненного *цикла* для разработки безопасных программ, разработанная и применяемая компанией Microsoft, носит название **Security Development Life Cycle**

(SDLC).Основная идея *SDLC* – учитывать *требования безопасности* в течение всего жизненного *цикла разработки* программ, начиная с самых ранних этапов.

В течение всего *цикла разработки ПО*, начиная с самых ранних этапов (требования, спецификации, проектирование), необходимо постоянно предусматривать меры надежности и безопасности *ПО*, чтобы впоследствии не пришлось их встраивать в систему в "авральном порядке", что значительно увеличит *затраты*.

Необходимо заранее анализировать и **моделировать возможные угрозы и атаки** на *ПО* и разрабатывать меры их отражения.

Необходимы инструменты количественной *оценки рисков*, с точки зрения надежности и безопасности.

Необходимы специальные виды тестирования *ПО* – **security testing, fuzzy testing (fuzzing)** – тестирование подсистемы безопасности и тестирование на граничные или близкие к граничным значения параметров, имитирующее действия хакеров *по* подбору и взлому IP-адресов и других *компонент* компьютерной системы.

Необходимы **эксперты по безопасности ПО (security buddies)**,участвующие в разработке в течение всего *цикла*.

Компания Microsoft предложила ряд простых схем для оценки и разработки безопасного программного обеспечения , для оценки угроз и атак и оценки последствий атаки, которые мы и рассмотрим.

Схема (формула) **SD3C** определяет основные принципы разработки безопасного программного обеспечения:

- **Secure in Design –** применение принципов безопасного проектирования; учет возможных атак; реализация способов их отражения;
- **Secure by Default –** включение установок безопасности по умолчанию;
- **Secure in Deployment –** безопасное развертывание и инсталляция программного обеспечения;
- **Communication –** постоянное взаимодействие группы сопровождения продукта с пользователями, быстрый выпуск новых версий продукта с исправленными ошибками безопасности; рекомендации по настройке безопасности.

Классификация угроз и атак (STRIDE)

По формуле STRIDE Microsoft предлагает классифицировать угрозы и атаки:

Spoofing – букв.: **пародирование, розыгрыш** – "подделка" под определенного пользователя; например, воспроизведение транзакции, выполняющей *аутентификацию пользователя*.

Tampering – Несанкционированное изменение данных с *целью атаки*; например, модификация аутентификационных файлов с целью добавления нового пользователя.

Repudiation – буквально означает **категорическое несогласие, отрицание, отказ** – отсутствие фиксации в системных журналах действий, которые могут привести к нарушению безопасности. В операционной системе *драйвер* может быть подвержен *repudiation*-угрозе, если он не выполняет *журналирование* (*logging*) действий, которые могут привести к нарушению безопасности. Например, *драйвер* видеоустройства, который не фиксирует запросы

на изменение фокуса и уменьшение размеров изображения (что может привести к его искажению).

Information disclosure – несанкционированный *доступ* к *конфиденциальной информации*; например: Получение списка номеров кредитных карт клиентов банка.

Denial of service – *Отказ в обслуживании*; например: сознательное достижение эффекта излишней *загрузки процессора*, используя недостатки хеш-алгоритма.

Elevation of privilege – Увеличение привилегий (несанкционированное *присваивание* прав системного администратора). Пример: *запуск* привилегированной программы для выполнения Ваших команд.

Оценка атак на программное обеспечение

Еще одна формула – **DREAD** – рекомендуется для оценки внешних атак:

Damage – *Ущерб*, нанесенный атакой.

Reproducibility – Воспроизводимость атаки: как часто она происходит и может ли быть воспроизведена (смоделирована).

Exploitability – здесь: квалификация (уровень); *опыт* и квалификация (хакера), необходимые для атаки.

Affected users – Против каких пользователей направлена *атака*.

Discoverability – Может ли *атака* быть обнаружена.

Борьба с атаками

Для борьбы с атаками могут быть предусмотрены следующие меры.

Проверка на подозрительные примеры активности – например, несколько подряд попыток ввести неверный *пароль* могут означать попытку его угадать.

Ведение **журнала аудита (audit log)** – в него записывается время, *пользователь* и тип каждой попытки доступа к объекту. Журнал используется для восстановления при нарушении защиты и для выработки более действенных мер безопасности.

Периодическое сканирование системы на предмет "дыр" в системе безопасности. Выполняется в моменты, когда *компьютер* практически не используется (пример - сканирование на вирусы).

Проверки на:

- Короткие или простые для угадывания пароли
- Несанкционированные программы, устанавливающие другие имена пользователей
- Несанкционированные программы в системных директориях
- Неожиданно долгие по времени процессы
- Неверную защиту директорий
- Неверную защиту системных файлов данных
- Опасные элементы в путях для поиска программ (ведущие к *троянским программам*)

- Изменения в *системных программах*: проверки *контрольных сумм*.

Брандмауэр

Брандмауэр (firewall) – системное программное обеспечение для защиты локальной сети от внешних атак. Брандмауэр помещается между "доверенными" и "не доверенными" компьютерами – например, компьютерами данной локальной сети и всеми остальными. Брандмауэр ограничивает сетевой доступ между двумя различными доменами безопасности. Встроенный брандмауэр имеется во всех современных операционных системах и по умолчанию включен. Настоятельно рекомендуется не отключать его, что особенно существенно при выходе в Интернет. Реализация брандмауэров, как правило, основана на фильтрации сетевых пакетов, пересылаемых с "надежных" и потенциально ненадежных IP-адресов.

Обнаружение попыток взлома

Действенной мерой безопасности является обнаружение попыток входа в компьютерные системы. Методы обнаружения:

- Аудит и ведение журнала (см. раздел **Борьба с атаками**);
- Использование **tripwire** - программ для UNIX, которые проверяют, не изменялись ли некоторые файлы и директории, например, файлы, содержащие пароли;
- Слежение за системными вызовами.

Криптография

Криптография – это преобразование понятного текста в зашифрованный текст. Методы криптографии широко используются для защиты *конфиденциальной информации*.

Свойства хороших методов криптования:

- Относительно простой для авторизованных пользователей способ криптования и декриптования данных.
- Схема криптования должна зависеть не от секретного алгоритма, а от секретного параметра алгоритма, называемого **ключом криптования** (**encryption key**).
- Для несанкционированного пользователя должно быть крайне сложно определить ключ.

Технология **Data Encryption Standard (DES)** основана на подстановке символов и изменении их порядка на основе ключа, предоставляемого авторизованным пользователям через защищенный механизм. Такая схема лишь настолько безопасна, насколько безопасен сам механизм получения ключа.

Криптование на основе открытого ключа – другой широко распространенный метод криптографии - основано на принципе, при котором пользователю известны два ключа:

public key – открытый ключ для криптования данных.

private key – закрытый ключ,известный только пользователю и применяемый им для декриптования данных.

Метод *открытого ключа* воплощает еще одно важное требование к методам криптографии: метод должен быть основан на схеме криптования, которая публично доступна, но это не будет облегчать разгадывание схемы декриптования.

Примером криптования, используемым в Web-технологиях, является **SSL (Secure Socket Layer)** - семейство криптографических протоколов, предназначенное для обмена криптованными сообщениями через *сокет*. *SSL* используется для защищенного взаимодействия между Web-серверами и браузерами (например, ввода номеров кредитных карт). При обращении клиента к серверу последний проверяется с помощью сертификата. Взаимодействие между компьютерами использует криптографию на основе *симметричного ключа*.

Уровни безопасности компьютеров

Министерство обороны США классифицирует *безопасность* компьютеров *по* уровням: A, B, C, D.

Уровень безопасности D соответствует минимальному уровню безопасности.

На **уровене безопасности C** обеспечиваются периодические проверки компьютера с помощью аудита. Уровень C подразделяется на уровни C1 и *C2*. **Уровень C1** обозначает взаимодействие пользователей с одинаковым уровнем безопасности. **Уровень C2** допускает *управление доступом* на уровне пользователей.

Уровень безопасности B имеет все свойства уровня C, однако каждый *объект* может иметь уникальные **метки чувствительности (sensitivity labels)**.Подразделяется на уровни B1, B2, B3.

На **уровне безопасности A** используются формальные методы спецификации и проектирования для обеспечения безопасности.

Безопасность в Windows NT

Конфигурируемое обеспечение безопасности допускает политики уровней от D до *C2* (*управление доступом* на уровне пользователей).

Безопасность основана на учетных записях пользователей, причем каждый *пользователь* имеет свой **идентификатор безопасности (security ID)**.

Используется субъектная модель для обеспечения безопасности доступа. Субъект отслеживает полномочия и управляет полномочиями для каждой программы, которую запускает *пользователь*.

Каждый *объект* в *Windows* NT имеет свой *атрибут* безопасности, определяемый **дескриптором безопасности (security descriptor)**.Например, *файл* имеет *дескриптор* безопасности, который задает полномочия доступа для всех пользователей.

Безопасность в .NET

Из всех систем и платформ для *разработки программного обеспечения*, в *.NET механизмы безопасности* наиболее развиты. *.NET* предоставляет гибкую, конфигурируемую систему безопасности. Имеется три основных вида организации и проверок безопасности.

Code Access Security (безопасность доступа к коду) – *конфигурирование* и проверки безопасности для *исполняемого кода* (сборки). Проверки безопасности осуществляются при исполнении программы на стеке текущего потока. Полномочия безопасности (например, разрешение на *открытие файла*) проверяются не только для конкретного вызванного метода, но и для всех методов всех сборок, вызванных на стеке текущего потока. Если хотя бы для одного из них полномочия нарушены, *программа* прекращается генерацией исключения **SecurityException**.Такая схема позволяет исключить атаки типа **elevation of privilege**.

Evidence-Based Security (безопасность, основанная на свидетельствах) – схема безопасности для проверки доверия к вызываемой двоичной сборке. Термин **evidence (свидетельство)** в данном случае означает информацию о сборке, которую анализирует система поддержки выполнения, - например, наличие цифровой подписи, компания-разработчик и др. На основе этого анализа определяется базовый набор полномочий сборки.

Role-Based Security (безопасность, основанная на ролях) – схема для гибкого конфигурирования полномочий безопасности пользователей. Каждому пользователю может быть приписана **роль** (обозначаемая *символьной строкой*, например, **"manager")**,с которой может быть связан определенный набор полномочий безопасности.

Атрибуты безопасности. В *.NET* широко используется понятие **атрибута** – произвольной информации, аннотирующей именованную сущность (например, *класс*, метод или *поле*). В частности, имеется встроенная система атрибутов безопасности. Атрибуты безопасности проверяются при загрузке сборки в *виртуальную машину* времени выполнения.

Декларативное и императивное управление безопасностью. Атрибуты безопасности являются **декларативным** методом управления безопасностью. Другой метод, **императивный**, заключается в вызове системных методов (например, **Demand**), проверяющих полномочия безопасности во *время выполнения*.

Ключевые термины

Data Encryption Standard (DES) – технология криптования, основанная на подстановке символов и изменении их порядка на основе ключа, предоставляемого авторизованным пользователям через защищенный механизм.

DREAD (*Damage, Reproducibility, Exploitability,* Affected users, Discoverability) – формула корпорации Microsoft для определения последствий атак.

Elevation of privilege – попытка расширить полномочия (например, до полномочий системного администратора) с целью злонамеренных действий.

Pharming – перенаправление пользователя на злонамеренный Web-*сайт* (обычно с целью **phishing**).

Phishing – попытка украсть *конфиденциальную информацию* пользователя путем ее обманного получения от самого пользователя (например, с помощью тревожного электронного письма).

SDLC (Security Development Life Cycle) – схема жизненного *цикла разработки* безопасных программ, предложенная и применяемая фирмой Microsoft.

SD3C (Secure in Design, by Default, in Deployment, and Communication) – формула требований к безопасности программного продукта фирмы Microsoft.

Spoofing – " подделка" под определенного пользователя, злонамеренное применение его логина, пароля и полномочий.

SSL (Secure Socket Layer) - семейство криптографических протоколов, предназначенное для обмена криптованными сообщениями через *сокет*.

STRIDE (Spoofing, Tampering with data, Repudiation, Denial of service, Elevation of privilege) – формула компании Microsoft для определения видов атак.

Tampering with data – *атака* путем искажения или порчи данных.

Tripwire - *системные программы* (для *UNIX*), проверяющие, не изменялись ли некоторые файлы и директории, например, файлы, содержащие пароли.

Trustworthy Computing (TWC) Initiative – инициатива корпорации Microsoft (2002), направленная на *улучшение* безопасности разрабатываемого кода.

Аутентификация (authentication) – *идентификация пользователей* при входе в систему.

Безопасность (security) – защита от внешних атак.

Брандмауэр (firewall) – системное *программное обеспечение* для защиты локальной сети от внешних атак, как бы образующее стену между "*доверенными*" и "не *доверенными*" компьютерами.

Вирус – фрагмент кода, встраивающийся в обычные программы с целью нарушения работоспособности этих программ и всей компьютерной системы.

Вход в ловушку (Trap Door) – *атака* путем использования логина или пароля, который позволяет избежать проверок, связанных с безопасностью.

Журнал аудита (audit log) – *системный журнал* подсистемы безопасности, в который записывается время, *пользователь* и тип каждой попытки доступа к *системным объектам* и структурам.

Закрытый ключ (private key) – *ключ*, известный только пользователю и применяемый им для декриптования данных.

Ключ криптования (**encryption key**) **–** секретный *параметр* алгоритма криптования, от которого зависит результат его работы.

Криптование на основе открытого ключа – метод криптографии, основанный на использовании пары ключей: на принципе, при котором пользователю известны два ключа: **открытый ключ** для криптования данных и **закрытый ключ** для декриптования данных.

Криптография – преобразование понятного текста в зашифрованный текст с целью защиты информации.

Логин (login, loginname) – зарегистрированное *имя пользователя* для входа в систему.

Отказ в обслуживании (Denial of Service – DoS) – *атака* на *сервер* путем создания его искусственной перегрузки с целью препятствовать его нормальной работе.

Открытый ключ (**public key) –** *ключ*, известный всем пользователям, и используемый для криптования данных.

Пароль (password) – секретное *кодовое слово*, ассоциируемое и вводимое в секретном режиме вместе с **логином**.

Переполнение буфера (Buffer Overrun) – *атака* путем использования ошибки в программе (*переполнения буфера* в памяти) для обращения к памяти другого пользователя или процесса с целью нарушения ее целостности.

Троянская программа (Trojan Horse) – атакующая *программа*, которая "подделывается" под некоторую полезную программу, но при своем запуске злонамеренно использует свое окружение, например, получает и использует *конфиденциальную информацию*.

Червь (Worm) – злонамеренная *программа*,
использующая *механизмы* самовоспроизведения (размножения) и распространяющаяся через *сеть*.