Введение и основные понятия.

Безопасность – защищенность ресурса от определенного множества потенциальных угроз.

Явление – состояние защищенности ресурса

Процесс – деятельность по защите ресурса от заданного множества угроз.

Информация – сведения, воспринимаемые субъектом в форме знаний.

Информация в современном обществе – это ресурс.

Угроза – потенциально возможное действие или событие, которое может привести к нарушению безопасности – нанести неприемлемый ущерб субъектам информационных отношений.

Субъекты информационных отношений – владелец информационного ресурса, потребитель информационного ресурса.

Уязвимость – свойство информационной системы, предоставляющее возможность реализации угроз безопасности, обрабатываемой в ней информации.

Потенциально «слабое место», ошибка в проектировании или реализации системы, которая может привести к неожиданным и нежелательным последствиям нарушения информационной безопасности.

Атака – попытка покушения на безопасность системы. Это действие (последовательность действий), которое может нарушить безопасность системы

Эксплойт – известный способ нарушения безопасности ИС, использующий ту или иную уязвимость.

Информационная безопасность в узком смысле слова - Защищенность национальных интересов в информационной сфере, определяемая совокупностью сбалансированных интересов личности, общества или государства.

Составляющие информационной безопасности:

- конфиденциальность – свойство информации, которое заключается в неизвестности информации третьим лицам.
- целостность – свойство информации, которое заключается в непротиворечивости информации, в невозможности несанкционированной модификации информации.

Виды целостности:

1. Статическая – неизменность информации в процессе хранения
2. Динамическая – корректное выполнение транзакций, корректная передача информации по каналам связи.

- Доступность – возможность для законных пользователей за приемлемое (установленное соответствующими нормами) время получить доступ к информации, информационной услуге.

1. Идентификация – это процесс, с помощью которого можно отличить один объект/субъект от другого объекта/субъекта. Это присвоение уникальных меток объектам/субъектам с целью отличить один от другого.

2. Аутентификация – определение подлинности субъекта/объекта (действительно ли он тот, за кого себя выдается)

- Неотказуемость – невозможность отрицать факт совершения действия, участия субъекта в транзакции.
- Подотчетность – фиксация всех событий в ИС, имеющие смысл с точки зрения безопасности.

Цель: обеспечить базу фактов для проведения расследования возможных инцидентов, связанных с нарушением безопасности.

Угроза конфиденциальности – потенциально возможное действие или событие, которое может привести к нарушению конфиденциальной информации. (потенциальная)

Угроза целостности – потенциально возможное действие или событие, которое может привести к нарушению целостности информации (повреждение, уничтожение)

Угроза доступности – потенциально возможное действие или событие, в результате которого система может быть недоступна для законных пользователей в течение длительного периода времени (превышающего установленную норму задержки).

Функциональность – безопасность – легкость использования.

Классификация угроз ИБ

По природе возникновения:
1. Естественные (физические процессы природные явления).
2. Искусственные (деятельность человека)

По степени преднамеренности:
1. Не преднамеренные (ошибки).
2. Преднамеренные: (умышленные действия)

По источнику угроз:
1. Природа.
2. Человек.
3. Санкционированные программные/аппаратные средства.
4. Несанкционированные программные/аппаратные средства

По положению источника угроз:
1. вне контролируемой зоны,
2. в пределах зоны

По степени зависимости от активности ИС:
1. Независимо от активности.
2. Только в процессе активности

По степени взаимодействия на ИС:
1. Пассивные
2. Активные

По этапам доступа пользователей к ресурсам:
1. Угрозы, проявляющиеся на этапе доступа к ресурсам.
2. Угрозы, проявляющиеся после разрешения доступа к ресурсам (злоупотребление полномочиями).

По способу доступа к ресурсам ИС:
1. Стандартный путь получения доступа к ресурсам: незаконное получение пароля -> Маскировка под другого пользователя.
2. Нестандартный путь получения доступа к ресурсам: недокументированные возможности ИС.

Средства защиты информации

Средства защиты бывают формальные и неформальные:

Неформальные средства защиты — это всевозможные правила, морально-этические средства, нормативные средства, законы и т.д.

Формальные – это специальные технические средства и программное обеспечение

Разграничение помогает разграничить зоны ответственности при создании систем информационной безопасности, так как при общем руководстве защитой административный персонал реализует нормативные способы, а IT специалисты технические.

Основы информационной безопасности предполагают разграничение полномочий не только в части использования информации, но и в части работы с её охраной. Подобное разграничение полномочий требует и нескольких уровней контроля.

Неформальные средства защиты

Неформальные средства защиты группируются на нормативные, административные и морально-этические. На первом уровне защиты находятся нормативные средства, регламентирующие ИБ в качестве процесса в деятельности организации. Нормативные средства обеспечения ИБ представлены законодательными актами и нормативно распорядительными документами, которые действуют на уровне организации. В мировой практике при разработке нормативных средств ориентируются на стандарты защиты, основным из которых является документ ISO IEC 27000-2016. Данный стандарт предполагает опробованные методики, необходимые для внедрения ИБ. Авторы этих методик считают, что основа информационной безопасности заключается в системности и последовательной реализации всех этапов от разработки до постконтроля. Для получения сертификата, который подтверждает соответствия стандартам по обеспечению ИБ необходимо внедрить все рекомендуемые методики в полном объеме. Если нет необходимости получать сертификат в качестве базы для разработки собственных систем ИБ, допускается принять любую из более ранних версий стандарта или российских ГОСТов, имеющих рекомендательный характер.

По итогам изучения стандарта разрабатываются два документа, которые касаются безопасности информации. Основной, но менее формальный документ – это концепция ИБ предприятия, которая определяет меры и способы внедрения системы ИБ для информационных систем организации. Второй документ, который обязаны исполнять все сотрудники компании – это положение об ИБ, утверждаемое на уровне совета директоров или исполнительного органа. Кроме положения на уровне компании должны быть разработаны перечни сведений, составляющих коммерческую тайну, приложения к трудовым договорам, закрепляющие ответственность за разглашение конфиденциальных данных, а также другие стандарты и методики. Внутренние нормы и правила должны содержать механизмы реализации и меры ответственности. Чаще всего эти меры носят дисциплинарный характер.

К организационным и административным мерам по защите информационной безопасности относятся:

- архитектурно-планировочные решения, позволяющие защитить переговорные комнаты и кабинеты руководства от прослушивания
- установление различных уровней доступа к информации
- сертификация деятельности компании по международным стандартам
- сертификация отдельных аппаратно-программных комплексов
- аттестация субъектов и объектов на соответствие необходимым требованиям безопасности

- получение лицензий, необходимых для работы с защищенными массивами информации
- оформление системы запросов на допуск к интернету, внешней электронной почте и другим ресурсам
- получение электронной цифровой подписи для усиления безопасности финансовой и другой информации, которую передают государственным органам по каналам электронной связи.

Формальные или технические средства защиты

Формальные или технические средства защиты включают несколько групп:

1. Физические средства защиты – это механические, электрические, электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним.

2. Аппаратные средства защиты – это электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в информационные и телекоммуникационные системы.

3. Программные средства – это пользовательские и системные программы, предназначенные для решения частных и комплексных задач, связанных с обеспечением ИБ. Такие комплексные системы могут служить для предотвращения утечки информации, её переформатирования и перенаправления информационных потоков, а также обеспечивают защиту от инцидентов в сфере ИБ.

4. Специфические средства информационной безопасности – это различные криптографические алгоритмы, позволяющие шифровать информацию при её хранении и передаче. Преобразование информации может выполняться при помощи программных и аппаратных методов, работающих в корпоративных информационных системах.

Все средства, гарантирующие безопасность информации, должны использоваться в совокупности после предварительной оценки ценности информации и сравнении её со стоимостью ресурсов, затраченных на охрану. Поэтому предложения по использованию средств защиты должны формулироваться уже на этапе разработки систем, а утверждение должно производиться на том уровне управления, который отвечает за утверждение бюджетов.

Защита информации от копирования

Защита от копирования заключается в предупреждении возможностей несанкционированного снятия копии с информации, находящейся в оперативной памяти компьютера или на каком-либо диске, в целях злоумышленного её использования.

Под системой защиты программ от копирования понимается система, которая обеспечивает выполнение ею своих функций только при опознании некоторого уникального неподдающегося копированию элемента, называемого ключевым.

Системы защиты от копирования можно разделить на следующие группы:

1. Защита программы с использованием стандартного носителя.
2. Использование подхода SaaS, то есть переноса кода самих программ в облако и предоставление функционала этих программ как сервиса.
3. Отдельные средства защиты непосредственно кода приложения от копирования и использования в других программах.
4. Использование механизмов активации программного обеспечения, когда программа привязывается к железу компьютера, а разработчик генерирует код активации.

Программные средства защиты от копирования:

- инсталляция программ;
- регистрационный код;
- защита CD, DVD;
- невозможность работы без диска;
- сканирование сети;
- проверка серийных номеров в интернете.

Аппаратные меры защиты от копирования

- наличие аппаратных ключей;
- запись информации в неиспользуемых секторах;
- проверка расположения и содержимого «сбойных» секторов;
- проверка скорости чтения отдельных секторов;
- техподдержка (косвенная защита).

К основным функции, которые выполняют системы защиты программ от копирования, заключаются в следующем:

1. Идентификация – присвоение индивидуального трудно подделываемого признака той среды, из которой будет запускаться защищаемая программа.
2. Аутентификация – опознавание той среды, из которой поступает запрос на копирование защищаемой программы.

3. Регистрация санкционированного копирования.
4. Реагирование на попытки несанкционированного копирования.
5. Противодействие изучению алгоритмов работы системы защиты.

Методы реализации способа идентификации:
1. Нарушение последовательности секторов флэш-накопителя;
2. Изменение межсекторной дистанции;
3. Форматирование с разным кодом длины 0 или 1.

Трассировка- пошаговое выполнение программы

Реагирование на попытки несанкционированного копирования:
1. Отказ в исполнении запроса;
2. Предупреждение злоумышленника о более серьезных санкциях;
3. Уничтожение защищаемой программы (после первой попытки или после нескольких попыток).

Противодействие изучению алгоритмов работы системы защиты предусмотрено для того, чтобы воспрепятствовать злоумышленнику в изучении структуры и содержания реализованной на дискете системы защиты в целях её преодоления (нейтрализации).

Для обнаружения модифицированного кода традиционно применялись следующие методы
1. Подсчет контрольных сумм критических участков
2. Использование контрольной суммы всего кода для расшифровки некоторого фрагмента.
3. Многопроходная расшифровка кода с ключом, вычисляемым на основе контрольной суммы всего кода либо критического участка.
4. Использование корректирующих кодов, позволяющих определить местоположение контрольного байта.
5. Контроль времени выполнения критического участка по сравнению с эталонным временем.
6. Контроль относительного времени выполнения участка программы (относительно другого участка).

Разделение и организация контроля доступа

Доступ к файлам как частный случай доступа к разделяемым ресурсов.

Операционная система должна контролировать доступ к любым разделяемым ресурсам. При этом используется общая схема. Пользователи пытаются выполнить с разделяемым ресурсом определенные операции, а операционная система должна решать имеют ли пользователи на это право. Пользователи являются субъектами доступа, а разделяемые ресурсы – объектами. Пользователь осуществляет доступ к объектам ОС не непосредственно, а с помощью прикладных процессов, которые запускаются от его имени. Для каждого типа объектов существует набор операций, которые можно с ними выполнять. Система контроля доступа должна предоставлять средства для задания прав пользователей по отношению к объектам дифференцированно по операции. Во многих операционных системах реализованы механизмы, которые позволяют управлять доступом к объектам различного типа с единых позиций. Например, в операционных системах Unix устройства ввода-вывода представлены в виде специальных файлов, что позволяет при доступе к устройствам использовать те же атрибуты безопасности и алгоритмы, что и при доступе к обычным файлам и каталогам. В ОС Windows NT используется унифицированная структура, объект безопасности, которая создается не только для файлов и внешних устройств, но и для любых разделяемых ресурсов, такие как секции памяти, синхронизирующих примитивы, типа семафоров и мьютексов и т. д. Это позволяет использовать Windows NT для контроля доступа к ресурсам любого вида, общий модуль ядра, менеджер безопасности. В качестве субъектов доступа могут выступать как отдельные пользователи, так и группы пользователей. У каждого объекта доступа существует владелец. Владельцем может быть, как отдельный пользователь, так и группа пользователей. Владелец объекта имеет право выполнять с ним любые допустимые для данного объекта операции. Во многих операционных системах существует особый пользователь, который имеет все права по отношению к любым объектам системы, не обязательно являясь их владельцем. Это администратор системы, которому необходим полный доступ ко всем файлам и устройствам для управления политикой доступа.

Существует 2 основных подхода к определению прав доступа. 1. Избирательный доступ имеет место, когда для каждого объекта сам владелец может определить допустимые операции с объектами. Этот подход называется также произвольным доступом, т. к. позволяет администратору и владельцем объектам произвольным образом по их желанию. Между пользователями и группами пользователей в системах с избирательным доступом нет жестких иерархических отношений, т. е. взаимоотношений, которые определены по умолчанию и которые нельзя изменить. Исключение делается только для администратора, по умолчанию наделяемого всеми правами. Мандатный доступ (принудительный) - такой подход к определению прав доступа, при

котором система наделяет пользователя определенными правами по отношению к каждому разделяемому ресурсу в зависимости от того, к какой группе пользователь отнесен. От имени системы выступает администратор, а владельцы объектов лишены возможностей управлять доступа к ней по своему усмотрению. Все группы пользователей в такой системе образуют строгую иерархию, причем каждая группа пользуется всеми правами группы более низкого уровня иерархии, к которым добавляются права данного уровня. Членам какой-либо группы не разрешается предоставлять свои права членам групп более низких уровней иерархии. Мандатные системы доступа считаются более надежными, но менее гибкими, обычно они применяются в специализированных вычислительных системах с повышенными требованиями к защите информации. В универсальных ОС общего назначения используются как правило избирательные методы доступа.

Механизм контроля доступа

Вход пользователя в систему порождает процесс оболочку, который поддерживает диалог с пользователем и запускает для него другие процессы. Процесс-оболочка получает от пользователя символическое имя и пароль и находит по ним числовые идентификаторы пользователя и его групп. Эти идентификаторы связываются с каждым процессом, запущенным оболочкой для данного пользователя. Говорят, что процесс выступает от имени данного пользователя и данных групп пользователей, наиболее типичным случаем любой порождаемый процесс наследует идентификаторы пользователя и групп от процесса родителя. Определить права доступа к ресурсу — значит определить для каждого пользователя набор операций, которые ему разрешено применять к данному ресурсу. В разных ОС для одних и тех же типов ресурсов может быть определен свой список дифференцируемых операций доступа. Набор файловых операций ОС может состоять из большого количества элементарных операций, а может включать всего несколько укрупненных операций. В ОС семейства Unix используется укрупненный подход, в котором существует всего 3 операции с файлами и каталогами (читать, писать и выполнить). Но содержание этих операций зависит от того, к какому объекту они применяются. В Windows NT используется гибкий подход, здесь реализована возможность работы с операциями над файлами на двух уровнях. По умолчанию администратор работает на укрупненном уровне, это уровень стандартных операций, а при желании может перейти на элементарный уровень, т. е. уровень индивидуальных операций. В самом общем случае права доступа могут быть описаны матрицей доступа, в которой столбцы соответствуют файлам системы, строки всем пользователям, а на пересечении строк и столбцов указываются разрешенные операции.

Практически во всех ОС матрица прав доступа хранится по частям, т. е. для каждого файла или каталога создается так называемый список управления доступа ACL (Access Control list) в котором описываются права на выполнение операцией пользователей и групп пользователей по отношению к этому файлу или каталогу. Список управления доступа является частью характеристик файла или каталога и хранится на диске в соответствующей области. Обобщенно формат списка управления доступа можно представить в виде набора идентификатора пользователей и групп пользователей, в котором для каждого идентификатора указывается набор разрешенных операций над объектом. Список ACL состоит из элементов управления доступом при этом каждый элемент соответствует одному идентификатору. Список ACL с добавленным к нему идентификатором владельца называют характеристиками безопасности.

Листы возможностей, когда для каждого субъекта Si создается файл всех объектов, к которому данный субъект имеет доступ.

Недостатки дискреционной модели:

1. Не выдерживает атаки при помощи троянского коня
2. Проблема контроля распространения прав доступа к объекту, т.к. при передаче прав владельца другому пользователю, права могут распространяться независимо от первого владельца файла.

Организация контроля доступа в ОС Windows NT

Отличается высокой гибкостью, которая достигается за счет большого разнообразия объектов.

Система безопасности следит за выполнением тех или иных действий клиента при помощи трех основных механизмов.

Привилегия – разрешение на выполнение некоторым пользователем некоторого действия в отношении всей системы в целом. (устанавливать время, вход, выход и т. д.)

При входе пользователя в систему для него создается так называемый токен доступа, включающий идентификатор пользователя и идентификаторы всех групп, в которые входит пользователь. В токене так же имеется список управления доступом (ACL по умолчанию), который состоит из разрешений и применяется к создаваемым процессам объектам, а также список прав пользователя на выполнение системных действий. Все объекты, включая файлы, потоки, события, даже токены доступа, когда они создаются, снабжаются дескриптором безопасности. Дескриптор безопасности содержит список управления доступа ACL. Владелец объекта обычно пользователь, который его создал, обладает правом избирательного управления доступом к объекту, может изменять ACL объекта, чтобы позволить или не позволить другим пользователям осуществлять доступ к объекту. Встроенный администратор в Windows NT, в отличие от супер-пользователя Unix, может не иметь некоторых разрешений на доступ к объекту. Для реализации этой возможности идентификаторы администратора и группы администраторов могут входить в ACL, как и идентификаторы рядовых пользователей. Однако администратор все же имеет возможность выполнить любые операции с любыми объектами, так как он всегда может стать владельцем объекта, а затем уже как владелец получить полный набор разрешений. Однако вернуть владение предыдущему владельцу объекта администратор не может, поэтому пользователь всегда может узнать о том, что с его ресурсом работал администратор. При запросе процесса доступа к объекту Windows NT управление всегда передается монитору безопасности, который сравнивает идентификаторы пользователя и групп пользователей из токена доступа с идентификаторами, хранящимися в ACL объекта. В элементах ALC Windows NT могут существовать как списки разрешенных, так и списки запрещенных для пользователя операций. Система безопасности осуществляет проверку разрешений только при каждом открытии объекта, а не при каждом его использовании.

Для смены в некоторых ситуациях процессом своих идентификаторов в Windows NT используется механизм олицетворения. В Windows NT существуют простые субъекты и субъекты-серверы. Простой субъект – это процесс, которому не разрешается смена токена доступа и соответственно

смена идентификаторов. Субъект-сервер – это процесс, который работает в качестве сервера и обслуживает процессы своих клиентов, например, процесс файлового сервера. Поэтому такому процессу разрешается получить токен доступа у процесса клиента, запросившего у сервера выполнение некоторого действия и использовать его при доступе к объектам.

В Windows NT однозначно определены правила, по которым вновь создаваемому объекту назначается список ACL. Если исполняемый процесс во время создания объекта явно задает все права доступа к вновь создаваемому объекту, то система безопасности приписывает этот ACL объекту. Если же программа не снабжает объект списком ACL, а объект имеет имя, то применяется принцип наследования разрешений. Система безопасности просматривает ACL того каталога объектов, в котором хранится имя нового объекта. Некоторые из кодов ACL каталога объектов могут быть помечены как наследуемые. Это означает, что они могут быть приписаны к новым объектам, создаваемым в этом каталоге. В том случае, когда процесс не задал явно список ACL для создаваемого объекта, и объект каталог не имеет наследуемых элементов ACL, используется список ACL по умолчанию из токена доступа процесса. Наследование разрешений употребляется наиболее часто при создании нового объекта, и оно особенно эффективно при создании файлов, так как эти операции выполняются в системе наиболее часто.

Многоуровневая модель доступа

Многоуровневые модели доступа предполагают формализацию процедуры назначения прав доступа посредством использования так называемых меток конфиденциальности или мандатов, назначаемых субъектом и объектом доступа. Права доступа каждого субъекта и характеристики конфиденциальности каждого объекта отражаются в виде совокупности уровня конфиденциальности и набора категорий конфиденциальности. Таким образом при назначении прав доступа посредством использования меток конфиденциальности или мандатов используются формализованные процедуры. Основу реализации управления доступа составляют: формальное сравнение метки субъекта и метки объекта, которому запрошен доступ, далее принимается решение о предоставлении доступа на основе некоторых правил для того, чтобы противодействовать снижению уровню конфиденциальности защищаемой информации.

Данные могут передаваться субъектами, если выполняются правила

1. Данные могут передаваться субъектом самому себе (если X не меньше X)
2. Данные могут передаваться от субъекта A к субъекту C, если они могут передаваться от субъекта A к субъекту B, и от субъекта B к субъекту C.
3. Если X не больше У и У не больше X, то X=У

Многоуровневая модель доступа в современных системах защиты реализуется через мандатный контроль или мандатную политику.

В таких системах существует монитор обращения.

Монитор обращения – подсистема мандатного контроля, удовлетворяющая некоторым требованиям.

Существуют требования к мандатному механизму, которые состоят в следующем.

1. Каждому субъекту и объекту доступа должны сопоставляться классификационные метки, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни. Данные метки должны служить основой мандатного принципа разграничения доступа.
2. Система защиты при вводе новых данных в систему должна запрашивать и получать от санкционированного пользователя классификационные метки этих данные. При санкционированном занесении в список пользователей нового субъекта ему должны назначаться классификационные метки. Внешние классификационные метки, т.е. метки субъектов и объектов должны точно соответствовать внутренним меткам, т.е. меткам внутри системы защиты.
3. Система защиты должна реализовывать мандатный принцип контроля доступа ко всем объектам при явном и скрытом доступе со стороны

любого из субъекта. Субъект может читать объект только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объектов.

4. Субъект осуществляет запись в объект только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации.

Особенности:

1. Менее гибкое администрирование, но более простое
2. Самое важное достоинство управлять доступом к ресурсам, которые он создает.
3. Такая система запрещает пользователю или процессу, обладающему определённые уровнем доверие, получать доступ к информации, процессам или устройствам более защищенного уровня
4. Устойчива к атаке троянским конем
5. Такая модель создана, в основном, для сохранения секретности информации.

Научная криптография
30-е – 60-е годы

Требования к надежным шифрам:

- ключ генерируется для каждого сообщения (каждый ключ используется только один раз)
- ключ статически надежен (то есть вероятности появления каждого из возможных символов равны, символы в ключевой последовательности независимы и случайны)
- длина ключа равна и больше длины сообщения
- исходный (открытый) текст должен обладать некоторой избыточностью (что является критерием оценки правильности расшифровки)

легко сменяемый элемент – некоторая информация сравнительно малого размера...

криптоаналитической атакой называется любая попытка расшифровать шифротекст для получения открытого текста...

Электронная цифровая подпись (ЭЦП)

DoS и DDoS атаки

DOS и DDOS атака – это агрессивные внешние воздействия на вычислительные ресурсы сервера или рабочей станции, проводимое с целью доведения последних до отказа. Под отказом понимается не физический выход машины из стоя, а недоступность её ресурсов для добросовестных пользователей, то есть отказ системы в их обслуживании. Если такая атака проводится с одиночного компьютера, она классифицируется, как DoS атака, если с нескольких, то Distributed DoS (DDoS) атака, то есть распределенное доведение до отказа в обслуживании.

1 группа – перегрузка полосы пропускания

2 группа – атака на уровне протоколов

Методы:

- Предотвращение
- Фильтрация
- Блэкхолинг
- Наращивание ресурсов
- Рассредоточение
- Уклонение
- Активные ответные меры