Политика безопасности и ее принципы

Инструменты и механизмы информационной безопасности включают в себя процессы и процедуры ограничения и разграничения доступа, информационное скрытие; введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации); использование методов надежного хранения, преобразования и передачи информации; нормативно- административное побуждение и принуждение.

На практике современные технологии защиты информации основаны на различных базовых сервисах (таких, как аутентификация, обеспечение целостности, контроль доступа и др.), и используют различные механизмы обеспечения безопасности (такие, как шифрование, цифровые подписи, управление маршрутизацией др.), но одних технических средств недостаточно: необходима организационно-управленческая деятельность - организационное обеспечение информационной безопасности, которое представляет собой одно из четырех основных направлений работы в общей системе мер в сфере информационной безопасности, включающей в себя также разработку специализированного программного обеспечения, изготовление и использование специальных аппаратных средств и совершенствование криптографических (математических) методов защиты информации.

Политика безопасности определяется как совокупность документированных управленческих решении, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться **следующими принципами:**

- невозможность миновать защитные средства;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы;
- обеспечение всеобщей поддержки мер безопасности;
- адекватность (разумная достаточность);
- системность;
- прозрачность для легальных пользователей;
- равностойкость звеньев.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать, программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен **принцип простоты и управляемости информационной системы в целом и защитных средств в особенности**. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.

Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Принцип адекватности (разумная достаточность). Совокупная стоимость защиты (временные, людские и денежные ресурсы) должна быть ниже стоимости защищаемых ресурсов. Вряд ли деклассированный пролетарий потратит деньги на металлическую дверь, суперзамок и сигнализацию, если в квартире непропитые вещи можно пересчитать по пальцам.

Системность. Конечно, важность этого принципа проявляется при построении крупных систем защиты, но и в небольшой фирме не стоит забывать о важности системного подхода. Он состоит в том, что система защиты должна строиться не абстрактно (защита от всего), а на основе анализа угроз, средств защиты от этих угроз, поиска оптимального набора этих средств.

Прозрачность для легальных пользователей. Можно заставлять пользователей перед каждой операцией для надежной идентификации вводить 10-значный пароль, прикладывать палец к сканеру и произносить кодовую фразу. Но не разбегутся ли после этого сотрудники.

Равностойкость звеньев. Звенья - это элементы защиты, преодоление любого из которых означает преодоление всей защиты (например, окно и дверь в равной степени открывают вору путь в квартиру). Понятно, что нельзя слабость одних звеньев компенсировать усилением других. В любом случае прочность защиты (или ее уровня, см. ниже) определяется прочностью самого слабого звена.

Главными этапами построения политики безопасности являются следующие:

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