Основы ИБ

Тема 2. Организационно-правовая защита информации

Лекция 4. Организационные методы защиты информации. Понятие политики информационной безопасности

Важной частью системы защиты информации является ***комплекс организационных мер*** по защите информации.

Организационные меры защиты информации представляют собой комплекс административных и ограничительных мер, направленных на защиту информации путем регламентации деятельности персонала и порядка функционирования средств (систем). К основным организационным мероприятиям относятся:

– создание службы защиты информации;

– разработка организационно-распорядительных документов, необходимых для организации комплексной защиты информации;

– определение порядка доступа к защищаемым объектам;

– установление и оформление правил разграничения доступа;

– ознакомление сотрудников организации с перечнем защищаемой информации, организационно-распорядительной документации по работе с ней;

– обеспечение охраны объекта информатизации путем установления системы контроля доступа, постов охраны, ограждающих сооружений и т.п.

– управление системой защиты информации.

Организационно-административные методы защиты информации

– Выделение специальных защищенных помещений для размещения ЭВМ и средств связи и хранения носителей информации;

– выделение специальных ЭВМ для обработки конфиденциальной информации;

– организация хранения конфиденциальной информации на специальных промаркированных магнитных носителях;

– использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;

– организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации;

– организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной ин-

формации; установление запрета на использование открытых каналов связи для передачи конфиденциальной информации;

– разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта;

– защита в процессе обработки, хранения, передачи и использования информации;

– постоянный контроль за соблюдением установленных требований по защите информации.

Состав организационно-распорядительных документов, как правило, включает:

– перечень информации, подлежащей защите;

– документы, регламентирующие порядок обращения сотрудников предприятия с информацией, подлежащей защите;

– положения о структурных подразделениях предприятия;

– документы, регламентирующие порядок взаимодействия предприятия со сторонними организациями по вопросам обмена информацией;

– документы, регламентирующие порядок эксплуатации автоматизированных систем предприятия;

– планы защиты автоматизированных систем предприятия;

– документы, регламентирующие порядок разработки, испытания и сдачи в эксплуатацию программных средств;

– документы, регламентирующие порядок закупки программных и аппаратных средств (в т.ч. средств защиты информации);

– документы, регламентирующие порядок эксплуатации технических средств связи и телекоммуникации.

Помимо этого, ***СТР-К*** для обеспечения защиты конфиденциальной информации ***рекомендует следующее***:

– на период обработки защищаемой информации в помещениях, где размещаются ОТСС, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации;

– допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только с санкции руководителя учреждения (предприятия) или руководителя службы безопасности;

– в случае размещения в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации;

– по окончании обработки защищаемой информации или при передаче управления другому лицу пользователь обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ПЭВМ;

– изменение или ввод новых программ обработки защищаемой информации в АС должен осуществляться совместно разработчиком АС и администратором АС;

– при увольнении или перемещении администраторов АС руководителем учреждения (предприятия) по согласованию со службой безопасности должны быть приняты меры по оперативному изменению паролей, идентификаторов и ключей шифрования.

Все носители информации, используемые в технологическом процессе обработки информации, подлежат учету в том подразделении, которое является владельцем АС, обрабатывающей эту информацию. Учет можно осуществлять по карточкам, бумажным журналам или автоматизировано. Носители должны быть промаркированы.

Маркировка должна содержать:

– учетный номер носителя;
– дата;
– гриф секретности;
– номер экземпляра;
– подпись сотрудника, ответственного за ведение учета.

Ответственность за соблюдением в организации или компании организационных (административных) мер по защите информации лежит на руководителе, начальнике службы безопасности (информационной безопасности), системном (сетевом) администраторе.

2. Понятие политики информационной безопасности

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 це-

лостности, 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 кри-

тически 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.

Системность. Конечно, важность этого принципа проявляется при построении крупных систем защиты, но и в небольшой фирме не стоит забы-

вать 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.

Политика безопасности – это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерных систем (КС) от заданного множества угроз.

Политика безопасности является тем средством, с помощью которого реализуется деятельность в компьютерной системе организации. Вообще политика безопасности определяется используемой компьютерной средой и отражает специфические потребности организации.

Обычно КС представляет собой сложный комплекс разнородного, иногда плохо согласующегося между собой аппаратного и программного обеспечения: компьютеров, ОС, сетевых средств, СУБД, разнообразных приложений. Все эти компоненты обычно обладают собственными средствами защиты, которые можно согласовать между собой. Поэтому в качестве согласованной платформы по обеспечению безопасности корпоративной системы очень важна эффективная политика безопасности. По мере роста компьютерной системы и интеграции ее в глобальную сеть, необходимо обеспечить от-

сутствие в системе слабых мест, поскольку все усилия по защите информации могут быть обесценены лишь одной оплошностью.

Политику безопасности нужно построить таким образом, чтобы она устанавливала, кто имеет доступ к конкретным активам и приложениям, какие цели и обязанности будут иметь конкретные лица, а также предусмотреть процедуры безопасности, которые четко предписывают, как должны выполняться конкретные задачи безопасности. Особенности работы конкретного сотрудника могут потребовать доступа к информации, которая не должна быть доступна другим работникам. Например, менеджер по персоналу может иметь доступ к частной информации любого сотрудника, в то время как специалист по отчетности может иметь доступ только к финансовым данным их сотрудников, а рядовой сотрудник будет иметь доступ только к своей собственной персональной информации.

Политика безопасности определяет позицию организации по рациональному использованию компьютеров и сети, а также процедуры по предотвращению и реагированию на инциденты безопасности. В большой корпоративной системе может применяться широкий диапазон разных политик от бизнес-политик до специфичных правил доступа к наборам данных. Эти политики полностью определяются конкретными потребностями организации.

Структура политики безопасности организации

Обычно политика безопасности организации включает:

- базовую политику безопасности;
- специализированные политики безопасности;
- процедуры безопасности.

Базовая политика безопасности устанавливает, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать.

Нисходящий подход, реализуемый базовой политикой безопасности, дает возможность постепенно и последовательно выполнять работу по созданию системы безопасности, не пытаясь сразу выполнить ее целиком. Базовая политика позволяет в любое время ознакомиться с политикой безопасности в полном объеме и выяснить текущее состояние безопасности в организации, структура и состав политики безопасности зависит от размера и целей компании. Обычно базовая политика безопасности организации поддерживается набором специализированных политик и процедур безопасности.

Специализированные политики безопасности

Потенциально существуют десятки специализированных политик, которые могут применяться большинством организаций среднего и большого размера. Некоторые политики предназначаются для каждой организации, другие – специфичны для определенных компьютерных окружений.

С учетом особенностей применения специализированные политики безопасности можно разделить на две группы:

– политики, затрагивающие значительное число пользователей (политика допустимого использования, политика удаленного доступа к ресурсам сети, политика защиты информации, политика защиты паролей и др.);

– политики, связанные с конкретными техническими областями (политика конфигурации межсетевых экранов, политика по шифрованию и управлению криптоключами, политика безопасности виртуальных защищенных сетей VPN, политика по оборудованию беспроводной сети и др.).

Рассмотрим подробнее некоторые из ключевых специализированных политик.

Политика допустимого использования. Ее цель – установление стандартных норм безопасного использования компьютерного оборудования и сервисов в компании, а также соответствующих мер безопасности сотрудников для защиты корпоративных ресурсов и собственной информации.

Политика допустимого использования предназначена в основном для конечных пользователей и указывает им, какие действия разрешаются, а какие запрещены. Политика допустимого использования устанавливает:

– ответственность пользователей за защиту любой информации, используемой и/или хранимой их компьютерами;

– правомочность пользователей читать и копировать файлы, которые не являются их собственными, но доступны им;

– уровень допустимого использования электронной почты и Web-доступа.

Специального формата для политики допустимого использования не существует: должно быть указано имя сервиса, системы или подсистемы (например, политика использования компьютера, электронной почты, компактных компьютеров и паролей) и описано в самых четких терминах разрешенное и запрещенное поведение, а также последствия нарушения ее правил и санкции, накладываемые на нарушителя.

Политика удаленного доступа. Ее цель – установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании. Эта политика касается всех сотрудников, поставщиков и агентов компании при использовании ими для удаленного соединения с сетью компании ком-

пьютеров или рабочих станций, являющихся собственностью компании или находящихся в личной собственности.

***Политика удаленного доступа*:**

– намечает и определяет допустимые методы удаленного соединения с внутренней сетью;

– существенна в большой организации, где сети территориально распределены;

– должна охватывать по возможности все распространенные методы удаленного доступа к внутренним ресурсам.

Политика удаленного доступа определяет:

– какие методы разрешаются для удаленного доступа;

– ограничения на данные, к которым можно получить удаленный доступ;

– кто может иметь удаленный доступ.

Процедуры безопасности являются необходимым и важным дополнением политикам безопасности. Политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты. Процедуры безопасности определяют, как защитить ресурсы и каковы механизмы выполнения политики, т. е. как реализовывать политики безопасности.

По существу, процедуры безопасности представляют собой пошаговые инструкции для выполнения оперативных задач. Часто процедура является тем инструментом, с помощью которого политика преобразуется в реальное действие. Например, политика паролей формулирует правила конструирования паролей, правила о том, как защитить пароль и как часто его заменять, процедура управления паролями описывает процесс создания новых паролей, распределения, а также процесс гарантированной смены паролей на устройствах.

Рассмотрим несколько важных процедур безопасности, которые необходимы почти каждой организации.

Процедура реагирования на события является необходимым средством безопасности для большинства организаций. Организация особенно уязвима, когда обнаруживается вторжение в ее сеть или, когда она сталкивается со стихийным бедствием.

Практически невозможно указать отклики на все события нарушений безопасности, но нужно стремиться охватить основные типы нарушений, которые могут произойти. Например, сканирование портов сети, атака типа «отказ в обслуживании», компрометация хоста, НСД и др.

Данная процедура определяет:

– обязанности членов команды реагирования;

– какую информацию регистрировать и прослеживать;

– как обрабатывать исследование отклонений от нормы и атаки вторжения;

– кого и когда уведомлять;

– кто может выпускать в свет информацию, и какова процедура выпуска информации;

– как должен выполняться последующий анализ и кто будет в этом участвовать.

Процедура управления конфигурацией обычно определяется на корпоративном уровне или уровне подразделения. Эта процедура должна определить процесс документирования и запроса изменений конфигурации на всех уровнях принятия решений.

Процедура управления конфигурацией определяет:

– кто имеет полномочия выполнить изменения конфигурации аппаратного и программного обеспечения;

– как тестируется и инсталлируется новое аппаратное и программное обеспечение;

– как документируются изменения в аппаратном и программном обеспечении;

– кто должен быть проинформирован, когда случаются изменения в аппаратном и программном обеспечении.

Процесс управления конфигурацией важен, так как документирует сделанные изменения и обеспечивает возможность аудита; документирует возможный простой системы; дает способ координировать изменения так, чтобы одно изменение не помешало другому.

Политика безопасности определяет стратегию управления в области информационной безопасности, а также меру внимания и количество ресурсов, которые считает целесообразным выделить руководство.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для КС организации. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого конкретными документами специализированных политик и процедур безопасности.