4. ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ В АС

Организационная структура, основные функции службы компьютерной безопасности

Для непосредственной организации (построения) и эффективного функционирования системы защиты информации в АС может быть (а при больших объемах защищаемой информации - должна быть) создана специальная штатная служба защиты (служба компьютерной безопасности) [7].

Служба компьютерной безопасности представляет собой штатное или нештатное подразделение, создаваемое для организации квалифицированной разработки системы защиты информации и обеспечения ее функционирования.

Основные функции службы заключаются в следующем [7]:

- формирование требований к системе защиты в процессе создания АС;
- участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования АС;
- распределение между пользователями необходимых реквизитов защиты;
- наблюдение за функционированием системы защиты и ее элементов;
- организация проверок надежности функционирования системы защиты;
- обучение пользователей и персонала АС правилам безопасной обработки информации;
- контроль за соблюдением пользователями и персоналом АС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
- принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

Организационно-правовой статус службы защиты определяется следующим образом:

- численность службы защиты должна быть достаточной для выполнения всех перечисленных выше функций;
- служба защиты должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;
- штатный состав службы защиты не должен иметь других обязанностей, связанных с функционированием АС;
- сотрудники службы защиты должны иметь право доступа во все помещения, где установлена аппаратура АС и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;
- руководителю службы защиты должно быть предоставлено право запрещать включение в число действующих новые элементы АС, если они не отвечают требованиям защиты информации;
- службе защиты информации должны обеспечиваться все условия, необходимые для выполнения своих функций.

Естественно, все эти задачи не под силу одному человеку, особенно если организация (компания, банк и др.) довольно велика. Более того, службу компьютерной безопасности могут входить сотрудники с разными функциональными обязанностями. Обычно выделяют четыре группы сотрудников (по возрастанию иерархии):

- ***Сотрудник группы безопасности.*** В его обязанности входит обеспечение должного контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема АС имеет своего сотрудника группы безопасности.
- ***Администратор безопасности системы.*** В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (если в этом возникает необходимость) и за хранением резервных копий.
- ***Администратор безопасности данных.*** В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.
- ***Руководитель (начальник) группы по управлению обработкой информации и защитой***. В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами в подсистемах АС (при децентрализованном управлении).

Существуют различные варианты детально разработанного штатного расписания такой группы, включающие перечень функциональных обязанностей, необходимых знаний и навыков, распределение времени и усилий. При организации защиты существование такой группы и детально разработанные обязанности ее сотрудников совершенно необходимы [31].

Основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования комплексной системы защиты

Они включают:

- разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;
- мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде (по необходимости);
- периодически проводимые (через определенное время) мероприятия;
- постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

Разовые мероприятия

К разовым мероприятиям относят:

- общесистемные мероприятия по созданию научно-технических и методологических основ (концепции и других руководящих документов) защиты АС;
- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т.п.);
- мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и программных средств, документирование и т.п.);
- проведение спецпроверок всех применяемых в АС средств вычислительной техники и проведения мероприятий по защите информации от утечки по каналам побочных электромагнитных излучений и наводок;

- разработка и утверждение функциональных обязанностей должностных лиц службы компьютерной безопасности;
- внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, инструкции пользователей системы и т.п.) по вопросам обеспечения безопасности программно-информационных ресурсов АС и действиям в случае возникновения кризисных ситуаций;
- оформление юридических документов (в форме договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе, между участниками информационного обмена и третьей стороной (арбитражем, третейским судом) о правилах разрешения споров, связанных с применением электронной подписи;
- определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;
- мероприятия по созданию системы защиты АС и созданию инфраструктуры;
- мероприятия по разработке правил управления доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями организации с использованием АС, а также используемых при их решении режимов обработки и доступа к данным; определение перечня файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну, а также требования к уровням их защищенности от НСД при передаче, хранении и обработке в АС; выявление наиболее вероятных угроз для данной АС, выявление уязвимых мест процесса обработки информации и каналов доступа к ней; оценку возможного ущерба, вызванного нарушением безопасности информации, разработку адекватных требований по основным направлениям защиты);
- организацию надежного пропускного режима;
- определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;
- организацию учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;
- определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует и что при этом они должны делать);
- создание отделов (служб) компьютерной безопасности или, в случае небольших организаций и подразделений, назначение нештатных ответственных, осуществляющих единое руководство, организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы обработки информации;
- определение перечня необходимых регулярно проводимых превентивных мер и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса АС в критических ситуациях, возникающих как следствие НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий.

Периодически проводимые мероприятия

К периодически проводимым мероприятиям относят:

- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- анализ системных журналов, принятие мер по обнаруженным нарушениям правил работы;
- мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации;

· периодически с привлечением сторонних специалистов осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты. На основе полученной в результате такого анализа информации принимать необходимые меры по совершенствованию системы защиты;
· мероприятия по пересмотру состава и построения системы защиты.

Мероприятия, проводимые по необходимости

К мероприятиям, проводимым по необходимости, относят:

· мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;
· мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения (строгое санкционирование, рассмотрение и утверждение всех изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т.п.);
· мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т.д.).

Постоянно проводимые мероприятия

Постоянно проводимые мероприятия включают:

· мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т.п.).
· мероприятия по непрерывной поддержке функционирования и управлению используемыми средствами защиты;
· явный и скрытый контроль за работой персонала системы;
· контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования АС;
· постоянно (силами отдела (службы) безопасности) и периодически (с привлечением сторонних специалистов) осуществляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.

Перечень основных нормативных и организационно-распорядительных документов, необходимых для организации комплексной системы защиты информации от НСД

· документы, определяющие порядок и правила обеспечения безопасности информации при ее обработке в АС (план защиты информации в АС, план обеспечения непрерывной работы и восстановления информации);
· документы, определяющие ответственность взаимодействующих организаций (субъектов) при обмене электронными документами (договор об организации обмена электронными документами).

План защиты информации в АС должен содержать следующие сведения:

· описание защищаемой системы (основные характеристики защищаемого объекта): назначение АС, перечень решаемых АС задач, конфигурация, характеристики и размещение технических средств и программного обеспечения, перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в АС и требований по обеспечению доступности, конфиденциальности, целостности этих категорий информации, список пользователей и их полномочий по доступу к ресурсам системы и т.п.;
· цель защиты системы и пути обеспечения безопасности АС и циркулирующей в ней информации;
· перечень значимых угроз безопасности АС, от которых требуется защита и наиболее вероятных путей нанесения ущерба;
· основные требования к организации процесса функционирования АС и мерам обеспечения безопасности обрабатываемой информации ;
· требования к условиям применения и определение зон ответственности установленных в системе технических средств защиты от НСД;
· основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности АС (особые обязанности должностных лиц АС).

План обеспечения непрерывной работы и восстановления информации должен отражать следующие вопросы:

· цель обеспечения непрерывности процесса функционирования АС, своевременность восстановления ее работоспособности и чем она достигается;
· перечень и классификация возможных кризисных ситуаций;
· требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов и т.п.);
· обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования системы.

Договор о порядке организации обмена электронными документами должен включать документы, в которых отражаются следующие вопросы:

· разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;
· определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;
· определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т.п.);
· определение порядка разрешения споров в случае возникновения конфликтов.

Что же необходимо защищать и от чего надо защищаться?

Защищать необходимо всех субъектов информационных отношений от возможного материального или морального ущерба, который могут нанести им случайные или преднамеренные воздействия на компьютерную систему и информацию.

Защищаться необходимо от таких нежелательных воздействий, как ошибки в действиях обслуживающего персонала и пользователей системы, ошибки в программном обеспечении, преднамеренные действия злоумышленников, сбои и отказы оборудования, стихийные бедствия и аварии. Естественно на основе разумного анализа риска.

Предотвращать необходимо не только несанкционированный доступ к информации с целью ее раскрытия или нарушения ее целостности, но и попытки проникновения с целью нарушения работоспособности этих систем. Защищать необходимо все компоненты систем: оборудование, программы, данные и персонал.

Все усилия по обеспечению внутренней безопасности систем должны фокусироваться на создании надежных и удобных механизмов принуждения всех ее законных пользователей и обслуживающего персонала к безусловному соблюдению требований политики безопасности, то есть установленной в организации дисциплины прямого или косвенного доступа к ресурсам и информации.

Одним из важнейших аспектов проблемы обеспечения безопасности компьютерных систем является выявление, анализ и классификация возможных путей реализации угроз безопасности, то есть возможных каналов несанкционированного доступа к системе с целью нарушения ее работоспособности или доступа к критической информации, а также оценка реальности реализации угроз безопасности и наносимого при этом ущерба.

Предотвратить внедрение программных закладок можно только путем создания замкнутой программной среды, в которой должна быть исключена возможность использования инструментальных программ, с помощью которых можно было бы осуществить корректировку данных и программ на носителях и в памяти. Не должно быть программирующих пользователей, способных создать свои инструментальные средства (разработка и отладка программ должна производиться на компьютерах, не входящих в состав защищенной системы). Все используемые программы должны проходить предварительную сертификацию на предмет отсутствия в них закладок (с анализом всех исходных текстов, документации и т.д.). Все доработки программ также должны проходить сертификацию на безопасность. Целостность и неискаженность программ должна периодически проверяться путем проверки его характеристик (длины, контрольной суммы). Должен осуществляться постоянный контроль, исключающий внедрение программных закладок и распространение вирусов.

Известно большое число как традиционных, так и специфических для распределенных систем путей проникновения и НСД к информации. Нет никаких гарантий невозможности изобретения принципиально новых путей.

На аппаратно-программном уровне (уровне операционных систем) сложнее всего защититься от целенаправленных действий высококвалифицированных в области вычислительной техники и программирования злоумышленников, но именно к этому надо стремиться.

Как строить систему защиты, какие методы и средства можно при этом использовать?

Все известные меры защиты компьютерных систем подразделяются на: законодательные, морально - этические, административные, физические и технические (аппаратурные и программные). Все они имеют свои достоинства и недостатки.

Наилучшие результаты достигаются при системном подходе к вопросам безопасности компьютерных систем и комплексном использовании различных методов и средств их защиты на всех этапах жизненного цикла систем.

Основными универсальными механизмами противодействия угрозам безопасности, реализуемыми в конкретных средствах защиты, являются:

- идентификация (именование и опознавание), аутентификация (подтверждение подлинности) и авторизация (присвоение полномочий) субъектов;
- контроль (разграничение) доступа к ресурсам системы;
- регистрация и анализ событий, происходящих в системе;
- контроль целостности ресурсов системы.

Система защиты должна строиться эшелонированно в виде концентрических колец безопасности (обороны). Самое внешнее кольцо безопасности обеспечивается морально-этическими и законодательными средствами (неотвратимость возмездия за совершенное деяние). Второе кольцо безопасности представлено физическими и организационными средствами - это внешняя защита системы (защита от стихийных бедствий и внешних посягательств). Внутренняя защита (защита от ошибочных и умышленных действий со стороны персонала и законных пользователей) обеспечивается на уровне аппаратуры и операционной системы и представлена линией обороны, исключающей возможность работы посторонних с системой (механизм идентификации и аутентификации), и кольцами защиты всех ресурсов системы от неавторизованного использования (механизм разграничения доступа в соответствии с полномочиями субъекта). Механизмы регистрации событий и обеспечения целостности повышают надежность защиты, позволяя обнаруживать попытки преодоления других уровней защиты и своевременно предпринимать дополнительные меры, а также исключать возможность потери ценной информации из-за отказов и сбоев аппаратуры (резервирование, механизмы отслеживания транзакций). И, наконец, последнее кольцо безопасности представлено средствами прикладной защиты и криптографии.

Организационные меры должны выступать в качестве обеспечения эффективного применения других методов и средств защиты в части, касающейся регламентации действий людей.

Защиту, основанную на административных мерах, надо везде, где только можно, усиливать соответствующими более надежными современными физическими и техническими средствами.

Опыт создания систем защиты позволяет выделить следующие основные принципы построения систем компьютерной безопасности, которые необходимо учитывать при их проектировании и разработке:

- системность подхода;
- комплексность решений;
- непрерывность защиты;
- разумная достаточность средств защиты;
- простота и открытость используемых механизмов защиты;
- минимум неудобств пользователям и минимум накладных расходов на функционирование механизмов защиты.