УДК 004.056.53

ЗАЩИТА ИНФОРМАЦИИ ОТ УГРОЗ СО СТОРОНЫ ОБСЛУЖИВАЮЩЕГО ПЕРСОНАЛА

Артемов В.В., Галушко С.А.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, artemovdp@yandex.ru

В статье анализируются особенности решения проблемы защиты информации от так называемых легальных пользователей, обслуживающего персонала, крупномасштабных катастрофоустойчивых центров обработки данных. На основе обобщения ранее полученных результатов по конкретной реализации и проведенных дополнительных исследований формируются общие принципы построения и требовании к системотехнической и организационной составляющим системы защиты.

Ключевые слова – защита информации, модель нарушителя.

ОБЪЕКТЫ ЗАЩИТЫ

Для проектирования системы защиты автоматизированной информационной системы (АИС) необходимо определить объекты защиты, возможных нарушителей, а также изучить возможные угрозы, которые должна устранять система защиты. Следующим шагом является проектирование необходимой системы защиты информации (средств защиты). После этого специалисты по проблемам компьютерной безопасности анализируют проблему и определяют требования к системе защиты.

Объекты защиты в АИС можно разделить по их назначению на следующие основные составляющие:

- защищаемые данные (информация и/или программы) – данные, для использования которых и создавалась АИС;
- служебные данные (информация и/или программы) – данные, обеспечивающие возможность использовать защищаемые данные;
- технико-аппаратное обеспечение – оборудование, обеспечивающее возможность использовать защищаемые и служебные данные.

На крупномасштабных катастрофоустойчивых ЦОД возрастает важность предотвращения несанкционированного доступа к объектам защиты.

Во-первых, на таких центрах, как правило, функционирует несколько АИС и сконцентрированы данные, ущерб от потери которых в результате несанкционированного доступа существенно превышает ущерб, нанесенный отдельной АИС.

Во-вторых, катастрофоустойчивое построение ЦОД предполагает наличие двух площадок размещения технико-программных средств – основной и вспомогательной. Управление безопасностью такой конструкцией существенно отличается от традиционного построения ЦОД на одной площадке [2].

МОДЕЛЬ НАРУШИТЕЛЯ

Потенциальные нарушители в ЦОД могут быть отнесены к одной из следующих категорий лиц:

1. Конечные пользователи – лица, для информационной поддержки деятельности которых создавалась АИС, эксплуатируемая на данном ЦОД;
2. Администраторы и операторы – лица, организующие эксплуатацию ЦОД;
3. Программисты сопровождения – лица, обслуживающие программное обеспечения (ПО) ЦОД;
4. Инженеры сопровождения – лица, обслуживающие оборудование ЦОД;
5. Лица, разрабатывающие и поставляющие ПО и оборудование для эксплуатации ЦОД, – сотрудники фирм-разработчиков и фирм-поставщиков ПО и оборудования;
6. Посторонние лица, не относящиеся ко всем вышеперечисленным категориям [1].

Первые четыре категории – легальные пользователи, для которых определен конкретный порядок доступа к программно-техническим или информационным ресурсам АИС. Нарушение порядка доступа такими пользователями автоматически делает их нарушителями.

Конечные пользователи взаимодействуют с системой на прикладном уровне (в терминологии OSI – модели) прикладным программным обеспечением (ППО) АИС. На этом уровне определяются допустимые действия пользователя и доступные ему данные. Для этого нужно построить ППО таким образом, чтобы пользователь не имел физической возможности вносить изменение в программное обеспечение, тогда его действия будут полностью ограничены интерфейсом взаимодействия с системой, представленными функциональными полномочиями и полномочиями доступа к данным.

Создание надежной системы защиты от легальных пользователей достаточно сложная и робота, так как они отвечают за эксплуатацию прикладного и системного ПО, а также оборудования на всех уровнях. Эти лица по своим должностным обязанностям имеют возможность доступа к программам и данным на уровне ниже прикладного, поскольку легально допущены к аппаратному обеспечению (оборудованию) и системному ПО ЦОД. Поэтому предусмотренные на прикладном уровне средства разграничения доступа не могут контролировать их действия [2].

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

На возникновение угроз влияют внутренние (человеческий) факторы, а также внешние. В числе внутренних угроз можно указать следующие:

- нарушение работоспособности ЦОД;
- нарушение доступности передаваемой, обрабатываемой и хранимой информации в ЦОД;
- нарушение целостности ПО в ЦОД и достоверности информации в ЦОД;
- фальсификация информации в ЦОД;
- нарушение конфиденциальности информации хранящейся в ЦОД;
- неправомочное использование ресурсов ЦОД;
- нарушение нормативных требований к эксплуатации ЦОД.

Вот некоторые примеры возможности реализации подобных угроз легальными пользователями:

- невыполнение установленного регламента проведения работ, нарушение режима охраны, нарушение порядка допуска физических лиц к системе, неправильное или несвоевременное планирование действий в чрезвычайных ситуациях и т.п.;
- неправильные или неправомерные действия администраторов системы при ее настройке и в процессе сопровождения (применение пакетов модификации ПО; формировании системных архивов баз данных; резервном копировании информации АИС и служебной информации ЦОД; дефрагментации и сжатии оперативной базы данных и т.п.); программистов, сопровождающих системное программное обеспечение, а также инженеров, осуществляющих техническое обслуживание оборудования.

Внешние факторы – влияние различного рода катастроф – техногенных, стихийных бедствий, террористических актов (атаки хакеров) и т. д.

Такие воздействия могут привести к нарушению доступности и целостности информации (вплоть до ее полного уничтожения). Поэтому большое значение имеет правильный выбор аппаратно-программной платформы, на основе возможностей которой можно построить необходимую систему защиты информации. Для этого необходимо определить минимальные возможности, которым должны обладать системотехнические средства, чтобы позволить создать защищенную программную среду, а также определить состав и содержание организационно-технических мер защиты, которые совместно с этими возможностями позволят обеспечить предотвращение угроз со стороны легального пользователя.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Пользователи могут объединяться в группы, например по функциональной принадлежности и быть членом различных групп одновременно. В каждой группе назначается старший, который руководит и несет ответственность за действия членов группы. Управлять доступом к ресурсу возможно либо на уровне отдельного пользователя, либо группы пользователей. Каждый пользователь, как правило, определяется в системе персональным идентификатором, только ему известным паролем.

Чтобы механизм управления программным доступом работал эффективно он должен обладать способностью идентифицировать лицо, которое пытается получить доступ к системе, а затем проверить подлинность этой идентификации, используя идентификатор пользователя и пароль. Когда лицо определяется в СБ в качестве пользователя, ему присваиваются идентификатор и временный пароль. В любой момент пользователь может затребовать изменение пароля.

После идентификации и аутентификации пользователя СБ может контролировать и управлять взаимодействием между пользователем и системным ресурсом (файлы, магнитные носители, программы). СБ определяет, какие ресурсы могут быть доступны этому пользователю и тип разрешенного доступа (чтение, запись и т.д.) [1].

ЗАКЛЮЧЕНИЕ

Сформулированные в статье требования к системотехническим средствам построения системы, обеспечивающей защиту информации, могут быть полезными при проектировании крупномасштабных катастрофоустойчивых центров обработки данных и способствовать принятию обоснованных решений по выбору аппаратно-программной платформы их построения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Невский А.Г. практика управления информациооной безопасностью. ISACA.RU 2002. http://www.cobit.ru/security/Pubs/Pub5_AAM_ADT.htm.

2. Будзко В.И., Киселев Э.В. Проблемы защиты информации от легального пользователя// Тез. докл. первой общероссийской ежегодной научно-практической конференции «Защита информации» 17-20 сентября 2002 г.