УДК 004.056.52

С. И. Алешников, С. А. Дёмин
С. Б. Фёдоров, А. С. Фёдоров

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (ПРЕДПРИЯТИЯ) И ПУТИ ИХ РЕШЕНИЯ

Рассматриваются проблемы обеспечения информационной безопасности организации (предприятия). Их решение предполагает изучение форм, способов и методов выявления и предупреждения опасности в информационной сфере, а также организацию оптимального управления системой обеспечения информационной безопасности и рациональный выбор средств защиты конфиденциальной информации.

Problems of information security of the firm (manufacture) are considered. Their decision assumes studying of forms, ways and methods of revealing and the danger prevention in information sphere, and also the optimal control of system of maintenance of information security and a rational choice of protection tools of the confidential information.

Ключевые слова: информационные технологии, информационная безопасность, угрозы, объекты защиты, средства защиты, архитектура СЗИ.

Key words: information technology, information security, threats, objects of protection, a protection tools, architecture of the protection tools.

Введение

Развитие информационных технологий, а также их повсеместное проникновение в самые различные сферы деловой деятельности привело к тому, что компьютерная информация может иметь вполне определенную стоимость. Поэтому одна из важнейших проблем развития информационных технологий на предприятии и организации — надежное обеспечение информационной безопасности [1]. Ее решение — изучение форм, способов и методов выявления и предупреждения опасности в информационной сфере, а также управление информационной безопасностью на предприятии, выбор средств защиты.

Деятельность по защите охраняемой обладателем информации, в первую очередь, связана с предупреждением утечки конфиденциальной информации. Согласно указу Президента РФ [2] выделяют виды конфиденциальной информации: служебная тайна, персональные данные, тайна следствия и судопроизводства, адвокатская, нотариальная, коммерческая тайна, тайна сущности изобретения до момента опубликования, профессиональная тайна, тайна связи, банковская, врачебная, налоговая тайна. В качестве защищаемого субъекта мы будем рассматривать государственную организацию (предприятие).

1. Виды и особенности угроз информации при их обработке в компьютерных системах

Утечка охраняемой информации обычно становится возможной вследствие совершения нарушений режима работы с конфиденциальной информацией. Каналы утечки информации в информационных системах обработки конфиденциальных данных разобьем на группы.

К первой группе относят каналы, образующиеся за счет дистанционного скрытого видеонаблюдения или фотографирования, применения подслушивающих устройств, перехвата электромагнитных излучений и наводок и так далее.

Во вторую группу включают наблюдение за информацией в процессе обработки с целью ее запоминания, хищение ее носителей, сбор производственных отходов, содержащих обрабатываемую информацию, преднамеренное считывание данных из файлов других пользователей, чтение остаточной информации, то есть данных, остающихся на магнитных носителях после выполнения заданий, и так далее.

К третьей группе относят незаконное подключение специальной регистрирующей аппаратуры к устройствам системы или линиям связи, злоумышленное изменение программ таким образом, чтобы эти программы наряду с основными функциями обработки информации осуществляли также несанкционированный сбор и регистрацию защищаемой информации, злоумышленный вывод из строя механизмов защиты.

К четвертой группе относят несанкционированное получение информации путем подкупа или шантажа должностных лиц соответствующих служб, сотрудников, знакомых, обслуживающего персона или родственников, знающих о роде деятельности.

2. Управление информационной безопасностью организации

Обязательное условие решения проблемы обеспечения информационной безопасности — централизованное управление процессом обработки конфиденциальной информации, которое предусматривает [3]:

- координацию действий структурных подразделений предприятия по реализации политики обеспечения информационной безопасности организации (предприятия);
- сосредоточение совокупности корпоративных ресурсов предприятия на решении задач, предусмотренных указанным планом;
- контроль за своевременностью и полнотой выполнения политики информационной безопасности.

Цель управления информационной безопасностью — обеспечение безопасности информации и объектов инфраструктуры, сохранение конфиденциальности, целостности и доступности информации и единства информационного пространства компании. В задачи управления входят построение моделей нарушителей и угроз безопасности информационных ресурсов организации. В рамках управления формируются требования к подсистемам обеспечения защиты информации, используемым в организации (на предприятии), осуществляется

контроль их выполнения, разрабатываются планы долгосрочного и среднесрочного развития программы информационной безопасности, реализуется ряд других важных мероприятий, направленных на достижение требуемого уровня информационной безопасности.

К объектам защиты информации обычно относят:

- объекты информационной инфраструктуры, включающие программно-технические комплексы обработки и хранения информации;
- объекты автоматизированных систем управления (АСУ) и информационных систем (ИС), включающие: отдельные автоматизированные рабочие места (АРМ) и локальные вычислительные сети (ЛВС), серверные сегменты ИС и АСУ, программно-технические комплексы поддержания специализированных БД;
- системы документооборота.

В системах обеспечения информационной безопасности (СОИБ) выделяют три составляющие: организационную, нормативно-правовую и техническую. При этом наибольшее число проблем возникает при формировании технической составляющей. В процессе ее формирования следует реализовать ряд базовых принципов.

Один из важнейших — функциональная интеграция программно-технических комплексов защиты с программно-техническими комплексами передачи и обработки информации, имеющими собственные встроенные средства защиты с развитой функциональностью (ОС рабочих станций (РС) и серверов, активное сетевое оборудование).

Второй принцип — физическое или виртуальное разделение ЛВС и информационных ресурсов структурных единиц организации с жестким распределением прав доступа к ресурсам между персоналом.

Существенное сокращение затрат на внедрение СОИБ обеспечивает базовый принцип защиты ИС с использованием типовых комплексов технических средств защиты информации.

«Газинформсервис» — один из крупнейших в РФ системных интеграторов в области безопасности и разработчик уникальных программных продуктов. Сетевая система защиты информации (СЗИ) «Блокхост-сеть» компании предназначена для комплексной и многофункциональной защиты от несанкционированного доступа (НСД) информационных ресурсов локальных/сетевых РС и серверов, функционирующих под управлением ОС Windows 2000/XP/2003/2008R2/Vista/7. Система может применяться при создании автоматизированных систем до класса защищенности 1В включительно, в том числе информационных систем персональных данных до класса К1 включительно.

3. СЗИ от НСД «Блокхост-сеть К»

СЗИ «Блокхост-сеть К» — программно-технический СЗИ от НСД к информации и предназначено для комплексной и многофункциональной защиты информационно-программных ресурсов от НСД при работе в многопользовательских автоматизированных системах (АС) [4; 5]. Механизмы защиты позволяют администратору безопасности решать задачи:

- усиление защиты от НСД в систему;
- разграничение доступа пользователей к ресурсам;

- обеспечение гарантированного удаления информации;
- разграничение доступа к запуску программ;
- контроль целостности объектов файловой системы;
- контроль целостности реестра;
- очистка памяти после завершения работы приложений;
- контроль вывода информации на печать, маркировка документов;
- разграничение доступа пользователей к администрированию СЗИ;
- просмотр информационных сообщений СЗИ в ходе работы;
- контроль событий безопасности защищаемой информации.

Структурно «Блокхост-сеть К» состоит из клиентской части, где реализованы базовые механизмы защиты, и серверной части — сервера безопасности, устанавливаемой на АРМ администратора безопасности.

Клиентская часть защищает РС от НСД к информации и может работать как на автономной РС, так и на РС в составе сети. Через серверную часть выполняется централизованное управление удаленными РС. Настройка клиентской и серверной частей выполняется соответственно через локальную и серверную консоль администрирования. Локальная консоль администрирования позволяет выполнять настройку непосредственно на РС. Серверная консоль нужна для настройки тех же механизмов на удаленных РС с рабочего места администратора безопасности. Настройка механизмов защиты в обеих консолях идентична.

В состав СЗИ «Блокхост-сеть К» также входят дополнительные компоненты, реализованные в виде отдельных программных приложений:

- **модуль контроля целостности реестра** (автономный и сетевой варианты). Автономный вариант модуля устанавливается на защищаемые РС в составе ЛВС или работающие автономно, сетевой вариант — на АРМ администратора безопасности;
- **система развертывания**. Устанавливается на АРМ администратора безопасности и позволяет удаленно устанавливать клиентские части СЗИ с АРМ администратора безопасности;
- **программа обновления версии**. Устанавливается при обновлении «Блокхост-сеть» до «Блокхост-сеть К» на РС, а также на АРМ администратора безопасности (при обновлении сетевого варианта).

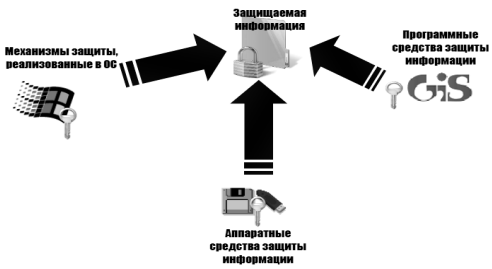

Рис. 1. Компоненты СЗИ

СЗИ «Блокхост-сеть К» дополняет функциональные возможности операционной системы по защите информации от несанкционированного доступа и защищает ее следующими компонентами (рис. 1).

В СЗИ «Блокхост-сеть К» реализован механизм двухфакторной аутентификации, который позволяет усилить защищенность входа РС за счет использования, помимо аутентификационных данных пользователя, персональных идентификаторов: eToken (USB-брелок или смарт-карта); JaCarta PRO; ruToken; USB-накопитель.

Механизм идентификации и аутентификации реализует функции:

- идентификацию и аутентификацию пользователя при входе;
- сопоставление пользователя с электронным идентификатором;
- запись пароля на парольный носитель и его считывание;
- блокирование и разблокирование системы;
- смену пароля пользователя.

Для идентификации и аутентификации пользователя при его входе в систему применяется два способа парольной защиты:

- вход в систему по паролю, вводимому с клавиатуры;
- вход в систему по ключевому носителю с паролем.

В СЗИ реализованы дискреционный и мандатные механизмы контроля доступа к информационным ресурсам, механизмы контроля печати, гарантированного удаления и очистки памяти и контроля целостности и гарантированного восстановления.

Механизм контроля печати осуществляет маркировку конфиденциальных документов, выводимых на печать, то есть вывод настраиваемого штампа в колонтитулах на страницах печатаемых документов.

Механизм гарантированного удаления запрещает удаление стандартным способом отмеченных файлов. Удаление файлов происходит трехкратным затиранием содержимого по алгоритму, исключающему считывание остаточной информации на диске после удаления.

Механизм очистки памяти очищает (обнуляет) освобождаемых СЗИ областей оперативной памяти и удаляемых данных на СЗИ.

Механизм контроля целостности проверяет целостность контролируемых файлов по алгоритму CRC-32 и при ошибке восстанавливает их. Этот же механизм используется для контроля целостности и надежного восстановления свойств СЗИ после сбоев и отказов оборудования.

Механизм контроля целостности реестра проверяет целостность разделов (ветвей), параметров (ключей) и значений параметров реестра Windows сравнением с эталоном и при ошибке информирует пользователя.

Общая архитектура «Блокхост-сеть К» представлена на рисунке 2.

Программную часть СЗИ «Блокхост-сеть К» можно разделить на ядро, выполняющее непосредственно функции защиты от НСД; программы, обеспечивающие пользовательский интерфейс; вспомогательные программные библиотеки и служебные программы (установка/удаление СЗИ «Блокхост-сеть К»).

Надежность защиты информации от НСД полностью определяется качеством работы ядра «Блокхост-сеть К». Протоколы взаимодействия ядра и остальной части ПО не допускают использования в составе ПО исполняемых кодов, модифицирующих коды и данные ядра.

Модуль аутентификации использует списки зарегистрированных пользователей и их пароли, хранимые в БД настроек СЗИ. Этот модуль начинает работать на последнем этапе загрузки ОС. Все попытки пройти аутентификацию записываются в журнал аудита.

Модуль диспетчера доступа — драйвер файловой системы и загружается до запуска графической оболочки ОС. Он запускается после прохождения пользователем аутентификации и начинает контролировать доступ к защищаемым объектам на основе информации из БД настроек СЗИ.

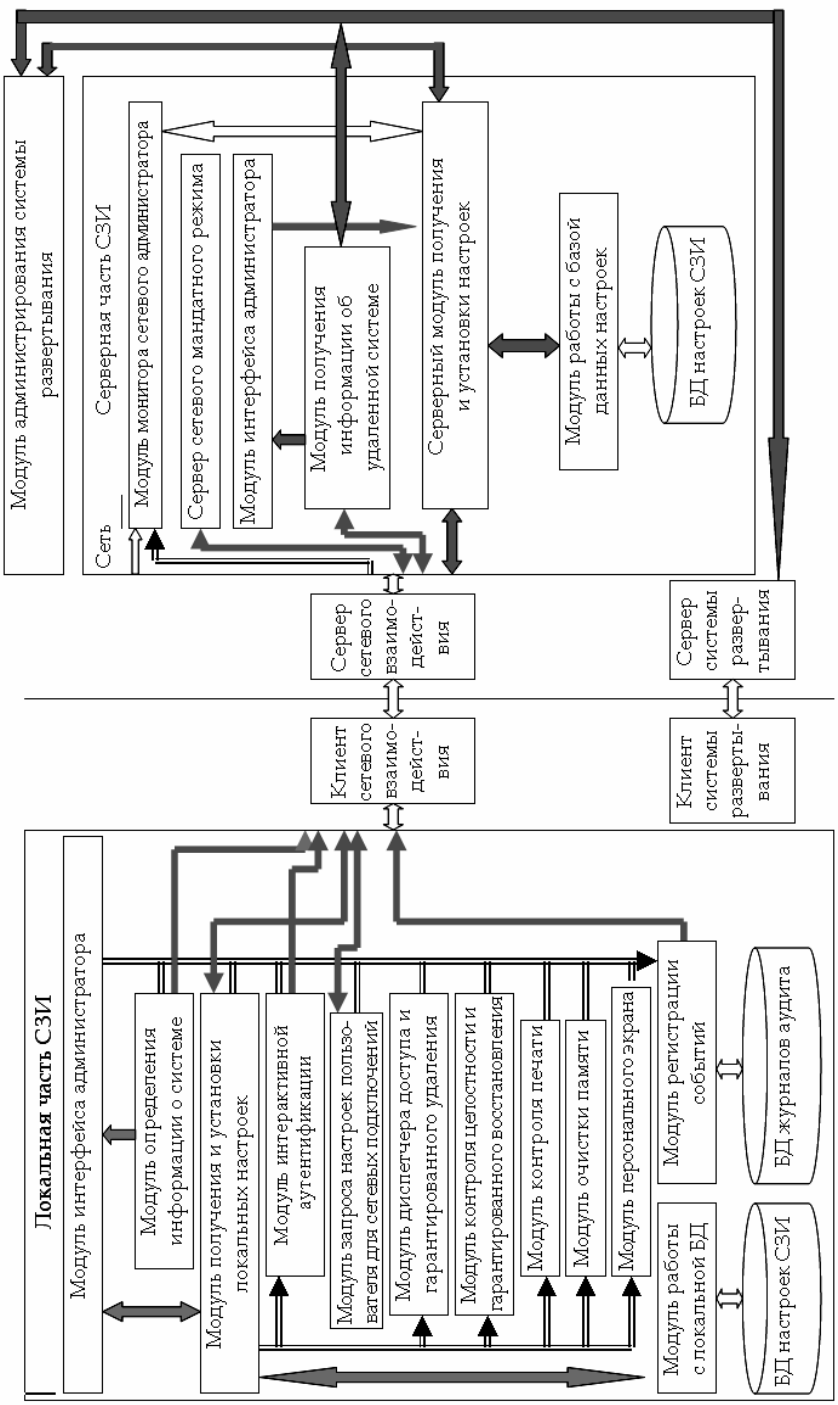

Рис. 2. Общая архитектура СЗИ

Модули контроля целостности и гарантированного восстановления и регистрации событий — сервисы Windows, запускаются при загрузке системы и постоянно находятся в памяти до перезагрузки компьютера.

Модуль персонального экрана загружается после драйвера NDIS, но до регистрации сетевых протоколов. Корректность проверки ЭЦП гарантирует целостность программной и информационной части ПЭ. Проверка ЭЦП осуществляется автоматически при запуске драйвера.

С помощью модуля интерфейса администратора (локального и серверного) производится настройка параметров системы защиты и сохранение их в БД настроек. Для того чтобы новые параметры вступили в силу, необходимо сменить сеанс пользователя.

Модуль определения информации о системе получает данные о локальных ресурсах машины, списках пользователей, текущих процессах и обслуживает запросы на получение данной информации как от локального модуля интерфейса администратора, так и удаленные.

Модуль получения информации об удаленной системе перенаправляет запросы о доступных ресурсах локальной машины модулю определения информации о системе данной локальной станции. Он обрабатывает информацию о подключении и отключении клиентских станций, информируя об этом модуль интерфейса администратора для разрешения/блокирования возможности их администрирования.

Модуль запроса настроек пользователя для сетевых подключений обрабатывает запросы модуля диспетчера доступа на загрузку настроек сетевых пользователей или запуска процессов от пользователя, не вошедшего интерактивно. Модуль обрабатывает запрос о текущем мандате пользователей на РС, что необходимо для сетевого мандатного режима.

Модуль очистки памяти контролирует работающие процессы и очищает память при завершении процесса, поставленного на контроль.

Модуль получения и установки настроек (локальный и серверный) — диспетчер, которому направляются запросы получения рабочих параметров при загрузке системы, входе пользователя или перезапуске модулей.

Модуль работы с БД (локальный и серверный) обрабатывает запросы на получение, сохранение настроек, кодирование и раскодирование файла конфигурации параметров работы системы и разграничений пользователей.

В модуль регистрации событий собираются все события аудита от модулей СЗИ. Затем производится фильтрация для выявления событий из заданного перечня, направляемых модулю монитора сетевого администратора для сигнализации о нарушениях безопасности.

Модуль контроля печати блокирует возможность печати на установленный виртуальный принтер и отслеживает отправку пользователем документа на другие установленные принтеры.

Модули клиента и сервера сетевого взаимодействия защищают удаленное управление разграничением полномочий пользователей на удаленных РС. Модуль монитора сетевого администратора сигнализирует о нарушениях безопасности, о подключении, о входе пользователей на РС.

Сервер сетевого мандатного режима хранит список работающих машин и мандаты вошедших пользователей, что необходимо для осуществления сетевого мандатного режима.

Список литературы

1. *Доктрина* информационной безопасности РФ [Электронный ресурс]: [Российская газета]. URL: http://www.rg.ru/oficial/doc/min_and_vedom/mim_ bezop/doctr. shtm (дата обращения: 10.08.2013).

2. *Об утверждении* Перечня сведений конфиденциального характера [Электронный ресурс]: указ Президента РФ от 06.03.1997 №188 [ред. №1111 от 23.09.2005] // Российская газета. 1997. №51. (дата обращения: 10.08.2013).

3. *Научные* и методологические проблемы информационной безопасности : сб. ст. М., 2004.

4. *Средство* защиты информации от несанкционированного доступа «Блокхост—сеть К». Руководство администратора безопасности. СПб., 2013.

5. *Средство* защиты информации от несанкционированного доступа «Блокхост—сеть К». Руководство пользователя. СПб., 2013.

Об авторах

Сергей Иванович Алешников — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: elliptec@mail.ru

Сергей Александрович Дёмин — ст. преп., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: sergeidemin@nm.ru

Сергей Борисович Фёдоров — начальник инспекции, Федеральная налоговая служба России, Калининград.
E-mail: elliptec@mail.ru

Александр Сергеевич Фёдоров — студ., Балтийский федеральный университет им. И. Канта, Калининград.
E-mail: elliptec@mail.ru

About the authors

Dr Sergey Aleshnikov — Ass. Prof., I. Kant Baltic Federal University, Kaliningrad.
E-mail: elliptec@mail.ru

Sergey Demin — high instructor, I. Kant Baltic Federal University, Kaliningrad.
E-mail: sergeidemin@nm.ru

Sergey Fedorov — chief of inspection, Federal Tax Service of Russia, Kaliningrad.
E-mail: elliptec@mail.ru

Alexandr Fjodorov — student, I. Kant Baltic Federal University, Kaliningrad.
E-mail: elliptec@mail.ru