УДК 004.056.53

В.С. Черненко

КОМПЛЕКС ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕРОПРИЯТИЙ, НАПРАВЛЕННЫЙ НА ЗАЩИТУ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРЕДПРИЯТИЯ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Черненко Вячеслав Сергеевич, *окончил Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики. Инженер 2 категории отдела информационных технологий ОАО «НПФ «Меридиан». [e-mail: slava2306@list.ru].*

Аннотация

В данной статье ставится задача защиты информации в автоматизированных системах предприятия от несанкционированного доступа. На примере защиты автоматизированной системы раскрывается комплексный подход к защите информации, показано совместное проведение организационных и технических мероприятий. В статье производится анализ автоматизированной системы предприятия, ее классификация, определение требований к ее защищенности. На основании анализа определяются специализированные средства защиты, а также организационные мероприятия, применимые к системе. В заключении раскрываются результаты применения данного подхода к защите.

Ключевые слова: несанкционированный доступ, утечка информации, защита информации, автоматизированные системы.

Введение

Одной из важнейших частей безопасности предприятия в настоящее время называют его информационную безопасность, обеспечение которой становится все более сложным и значимым процессом в связи с переходом информационных технологий на безбумажную автоматизированную основу. В современной рыночной экономике условием успеха организации в бизнесе и получения прибыли является обеспечение безопасности деятельности.

Безопасность информации – это не только защита от утечки, но и обеспечение ее сохранности, а также меры по защите важнейших данных от несанкционированного доступа (НСД) и обеспечению доступности информации в случае форс-мажорных обстоятельств.

Под информационной безопасностью понимают защиту субъектов информационных отношений. Основные ее составляющие: конфиденциальность, целостность, доступность.

Определение конфиденциальности дает 149-ФЗ «Об информации, информационных технологиях и о защите информации». Конфиденциальность – обяза-

тельное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [1]. Исходя из этого можно сделать вывод, что конфиденциальность и защита информации от НСД связаны между собой. Без защиты от НСД конфиденциальность попадает под угрозу. Данная статья посвящена решению задачи обеспечения защиты от НСД как важнейшей составляющей безопасности.

Безопасность информации определяется степенью ее защищенности от последствий форс-мажорных обстоятельств, а также попыток злоумышленника получить НСД к данным. В результате может произойти хищение и использование информации в преступных целях. Информационная безопасность не сводится только лишь к защите от НСД. Это более широкое понятие. Данные могут пострадать не только от НСД, но и от отказа системы, что в результате вызовет ее простой и, соответственно, потерю прибыли.

Таким образом, в связи с разнообразными видами угроз, на сегодняшний день задача защиты информации, в том числе и от НСД, более чем актуальна и является одной из самых важных в обеспечении непрерывной работы предприятия.

Для решения задач защиты информации от НСД в рамках данной статьи применяется комплексный подход, который совмещает в себе организационные и технические мероприятия.

В общем случае комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках соответствующей системы, условно состоящей из следующих подсистем:

– управления доступом;
– регистрации и учета;
– криптографической;
– обеспечения целостности [2].

В зависимости от класса автоматизированной системы (АС) в рамках этих подсистем должны быть реализованы соответствующие требования.

Классификация автоматизированной системы

При проведении комплекса мероприятий по защите информации от НСД для АС сначала необходимо ее классифицировать, для чего следует произвести аналитическое обследование, а затем реализовать для информации соответствующие требования. Классификация важна для более детальной разработки требований к защищенности АС.

Рассмотрим АС электронного документооборота на предприятии. Определим исходные данные для данной АС, а затем сформулируем и реализуем требования к ее защищенности.

Исходные данные:

– система обрабатывает конфиденциальную информацию;

– в системе одновременно хранится (или обрабатывается) информация различных уровней конфиденциальности;

– система не обрабатывает отнесенную к категории секретной или являющуюся собственностью государства информацию;

– система многопользовательская;
– пользователи имеют разные права доступа к информации;
– система обеспечивает коллективный режим обработки данных;
– не все пользователи имеют право доступа ко всей информации.

На основе исходных данных классифицируем систему по классу 1Г. В соответствии с классом защищенности 1Г система должна выполнять следующие требования (таблица):

Таблица

Требования к АС класса 1Г

Подсистемы и требования	Класс 1Г
1. Подсистема управления доступом	
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	
– к системе	+
– терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	+
– программам	+
– томам, каталогам, файлам, записям, полям записей	+
1.2. Управление потоками информации	=
2. Подсистема регистрации и учета	
2.1. Регистрация и учет:	
– входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	+
– выдачи печатных (графических) выходных документов	+
– запуска (завершения) программ и процессов (заданий, задач)	+
– доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	+
– доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	+
– изменений полномочий субъектов доступа	=
– создаваемых защищаемых объектов доступа	=
2.2. Учет носителей информации	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	+
2.4. Сигнализация попыток нарушения защиты	=

Продолжение таблицы	
Подсистемы и требования	Класс 1Г
3. Криптографическая подсистема	
3.1. Шифрование конфиденциальной информации	–
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	–
3.3. Использование аттестованных (сертифицированных) криптографических средств	–
4. Подсистема обеспечения целостности	
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+
4.3. Наличие администратора (службы) защиты информации в АС	–
4.4. Периодическое тестирование СЗИ НСД	+
4.5. Наличие средств восстановления СЗИ НСД	+
4.6. Использование сертифицированных средств защиты	–

Специализированные средства защиты

Для выполнения требований данного класса защищенности используются специализированные средства защиты, позволяющие защитить хранимую и обрабатываемую информацию. В данном случае используем средство защиты Security Studio Endpoint Protection, которое включает в себя:

– антивирус;
– межсетевой экран;
– средства обнаружения вторжений;
– антиспам;
– контроль интерактивных элементов веб-страниц.

Средство защиты позволяет обнаружить вторжения, предотвращает попытки вредоносного ПО проникнуть в компьютер, обеспечивает безопасный доступ к сети, обнаруживает шпионское ПО. Сертификация позволяет выполнить требования ФСТЭК по защите информации, обеспечивает защиту информации от НСД в АС по классу 1Г. Возможно использование в комплексе со средствами защиты информации от НСД Secret Net для защиты автоматизированного рабочего места.

В результате внедрения данного специализированного средства защиты обеспечивается защита автоматизированного рабочего места от НСД по сети, проникновений и утечек информации, а также не остаются незамеченными попытки злоумышленника проникнуть в систему.

«Панцирь-К» – комплексная система защиты информации, одно из лучших средств защиты информации от НСД. Система реализована программно и работает под операционными системами Windows 2000/XP/2003/VISTA/2008/7, не использует ни один входящий в операционные системы механизм защиты,

многие из которых имеют серьезные недостатки. Обеспечивает использование в АС по классу защищенности 1Г, применяется для защиты от внешних и внутренних угроз, эффективно противодействует возможным атакам. С помощью системы осуществляется коллективный доступ к зашифрованным данным в сети. Кроме того, система выполняет следующие функции, позволяющие соблюдать требования класса защищенности 1Г:

– производит разграничение доступа к локальным и сетевым ресурсам: принтеры, внешние накопители, файлы, объекты реестра операционной системы;
– осуществляет управление подключением устройств;
– производит противодействие атакам, расширяющим привилегии;
– противодействует закладкам и ошибкам в ПО;
– позволяет проводить авторизацию через аппаратные средства ввода пароля;
– производит контроль целостности данных;
– противодействует запуску троянов и программ-шпионов.

Система содержит клиентскую и серверную части, что позволяет администратору безопасности производить настройку системы безопасности и осуществлять пресечение попыток НСД в реальном времени.

В результате применения данной системы получаем разграничение прав доступа и контроль работы пользователей с локальными и сетевыми ресурсами, разграничение работы программ. Производится контроль рабочего времени пользователей. Применяется также шифрование данных, благодаря чему обеспечивается их защита от неправомерных действий сотрудников предприятия.

Таким образом, применяя комплексную систему защиты информации «Панцирь-К», мы получаем эффективное средство защиты информации от НСД, позволяющее решать ежедневные задачи защиты данных на предприятии и выполнять требования нормативных документов.

Организационные мероприятия

Техническим средствам защиты информации нужна непрерывная организационная поддержка, которая заключается в смене паролей, определении ролей, полномочий, разграничении доступа и т. п. То есть защита информации – это не разовое мероприятие, это постоянный процесс. Требуется обеспечить беспрерывность работы средств защиты, чтобы злоумышленники не смогли проанализировать систему безопасности и при случае воспользоваться возможными уязвимостями, заложить «закладки» или вывести систему из строя. Этого возможно добиться путем проведения следующих мероприятий на предприятии, в соответствии с классом защищенности, а также согласно руководящему документу:

– выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;

– определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;

– установление и оформление правил разграничения доступа, т. е. совокупности правил, регламентирующих права доступа субъектов к объектам;

– ознакомление субъекта доступа с перечнем защищаемых сведений и его

уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

– получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;

– обеспечение охраны объекта, на котором расположена защищаемая АС (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;

– выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

– организация службы безопасности информации (ответственные лица, администратор ИБ), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т. д.;

– разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;

– осуществление приемки СЗИ НСД в составе АС [2].

Планирование организационных мероприятий может осуществляться службой безопасности предприятия на разное время (год, месяц, а также на любой другой срок). Служба безопасности также занимается и разработкой организационно-распорядительных документов и контролирует их выполнение. Особое внимание уделяется допуску и доступу сотрудников предприятия к конфиденциальной информации, проверке носителей информации.

В результате проведение организационных мероприятий позволяет перекрыть большую часть каналов утечки информации и объединить используемые специализированные средства защиты в единый механизм.

Путем проведения организационных и технических мероприятий была достигнута цель в решении задачи защиты АС от НСД по классу защищенности 1Г. В результате выполняются все требования данной классификации. Совокупность организационных методов и специализированных средств защиты позволяет оперативно реагировать на угрозы в процессе хранения, обработки, передачи информации, а также обеспечивать ее доступность и целостность. Только при совместном их применении достигается наилучший результат.

По окончании проведения мероприятий по защите, а также в процессе эксплуатации АС проводится оценка эффективности средств защиты, при которой используется преимущественно системный подход. Важно помнить, что при этой оценке необходимо учитывать общие технические характеристики объекта защиты (включая практическую реализацию средств защиты), а также экономическую

сторону данного вопроса. Необходимо осуществлять контроль эффективности средств защиты от НСД, который может производиться либо периодически, либо по мере необходимости. В случае необходимости выполняется доработка средств защиты.

Заключение

Таким образом, при проведении организационных и технических мероприятий по защите информации предприятия от НСД результатом стал комплекс средств и методов защиты информации. Достигнута высокая степень защищенности по классу 1Г. Конечно же, стопроцентной гарантии на безопасность дать невозможно, так как при достаточном количестве времени и средств любая защита может быть преодолена, но избежать рисков все же можно, используя комплексный подход, описанный в рамках данной статьи.

Рекомендовано к применению для АС на предприятиях.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.