УДК 621.391(075.8)

Трещев Иван Андреевич
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Заведующий кафедрой «Информационная безопасность автоматизированных систем»
Кандидат технических наук
E-Mail: kalkt@yandex.ru

Защита от несанкционированного доступа к информации на предприятии

Аннотация. В данной работе проведен анализ организационно-распорядительных документов, которые должны быть на предприятии с целью защиты от несанкционированного доступа к конфиденциальной информации обрабатываемой в информационных системах. Проведен анализ сертифицированных программно-аппаратных средств защиты.

Ключевые слова: информационная безопасность; система защиты информации; угрозы безопасности.

Введение

Правовое обеспечение дает возможность урегулировать многие спорные вопросы, неизбежно возникающие в процессе информационного обмена на самых разных уровнях - от речевого общения до передачи данных в компьютерных сетях. Кроме того, образуется юридически оформленная система административных мер, позволяющая применять взыскания или санкции к нарушителям внутренней политики безопасности предприятия, а также устанавливать достаточно четкие условия по обеспечению конфиденциальности сведений, используемых или формируемых при сотрудничестве между субъектами экономики, выполнении ими договорных обязательств, осуществлении совместной деятельности и т. п. При этом стороны, не выполняющие эти условия, несут ответственность в рамках, предусмотренных как соответствующими пунктами межсторонних документов (договоров, соглашений, контрактов и пр.), так и российским законодательством [1]. В организации должен быть создан перечень документов для системы защиты информации:

- Перечень конфиденциальной информации и иных объектов, подлежащих защите от несанкционированного доступа в информационных системах;
- Положение о разграничении прав доступа к обрабатываемой конфиденциальной информации в информационных системах;
- Положение об ответственности сотрудников организации за разглашение конфиденциальной информации и несанкционированный доступ к ней;
- Положение о подразделениях;
- Должностная инструкция Пользователя информационной системы;
- Устав;
- Коллективный трудовой договор;
- Правила внутреннего распорядка служащих предприятия;
- Должностные обязанности руководителей, специалистов и служащих предприятия;
- Инструкции пользователей информационно-вычислительных сетей и баз данных;
- Инструкции сотрудников, допущенных к защищаемым сведениям;
- Инструкции сотрудников, ответственных за защиту информации.

Выбор в пользу тех или иных средств защиты информации при разработке информационных систем, обрабатывающих конфиденциальную информацию – ключевая процедура, определяющая не только будущий уровень защищенности и надежности системы, но и законность дальнейшей эксплуатации с точки зрения российского законодательства[2].

В соответствии с законодательством Российской Федерации, организационно-распорядительными и нормативными документами ФСТЭК и ФСБ России в государственных информационных системах, обрабатывающих конфиденциальную информацию, использование сертифицированных программных продуктов по требованиям информационной безопасности является обязательным.

Применение в информационной системе сертифицированных средств защиты не является достаточным условием выполнения требований законодательных и нормативных актов, важно чтобы параметры безопасности соответствовали требованиям Руководящих

документов к системе безопасности автоматизированных систем, но и могли быть подтверждены уполномоченным органами при аттестации объекта информатизации[3].

Если использование сертифицированных средств защиты информации не обязательно, то выбор в пользу сертифицированных средств защиты предпочтителен, поскольку наличие сертификата является важным фактором обеспечения доверия к приобретаемым программным продуктам, а так же гарантия безопасности и качества.

Выбор сертифицированного средства защиты информации зависит от класса автоматизированной системы, а так же от класса её защищенности и должен проводиться по результатам аудита информационной безопасности информационной системы предприятия[3].

Средства защиты от несанкционированного доступа (СЗИ от НСД) по своему исполнению можно разделить на программные и программно-аппаратные, а по сфере применения – для защиты конфиденциальной информации.

Для типового предприятия при выборе СЗИ от НСД были определены следующие требования:

- выполнение требований руководящих документов (РД) ФСТЭК;
- развитость функционала помимо требований РД;
- совместимость с другими продуктами по защите информации (антивирус, межсетевой экран, VPN и т.д.);
- простота внедрения (развертывания);
- стабильность работы и совместимость с приложениями;
- совместимость с ОС компьютера;
- слабое влияние на работоспособность компьютера в процессе работы;
- отсутствие дополнительных средств, затрудняющих установку и эксплуатацию;
- стоимость приобретения и внедрения.

В настоящее время среди всех сертифицированных СЗИ от НСД можно выделить следующие продукты:

- SecretNet и Соболь (Код Безопасности).
- Аккорд (ОКб САПР).
- Dallas Lock (НПП ИТБ).
- КРИПТОН (Анкад).
- СЗИ Аура (СПИИРАН).

Сравнение возможностей продуктов представлено в таблице 1.

Таблица 1

Сравнение СЗИ от НСД

Характеристика	Secret Net 6 (лок)	Аккорд	Dallas Lock 7.7	КРИПТОН	СЗИ Аура
Наличие сертификата по РД	да	да	да	да	да
Идентификация и аутентификация пользователей до загрузки ОС	да	да	да	да	да
Возможность аппаратной идентификации	да	нет	да	нет	да
Защита от обхода загрузки СЗИ	да	да	да	да	да
Контроль целостности до загрузки ОС	да	да	да	да	да
Обеспечение целостности информационной системы и информации	да	да	да	да	да
Автоматическая очистка дискового пространства при удалении информации	да	нет	да	нет	да
Зачистка дискового пространства при удалении произвольных файлов	да	да	нет	да	нет
Кодирование данных	да	нет	да	нет	да
Разграничение доступа к внешним носителям, устройствам	да	да	да	да	да
Контроль аппаратной конфигурации	да	да	частично	да	да
Интеграция с доменом в режиме рабочей станции домена	да	да	да	да	да
Регистрация событий безопасности	да	нет	да	нет	да
Совместимость с ОС Windows 7	да	нет	да	нет	да
Средняя стоимость, руб.	5100	9089	6000	6100	5900

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ[4], либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации

Межсетевой экран – комплекс аппаратных или программных средств, осуществляющих контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами[5].

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа.

На типовом предприятии для системы, осуществляющей межсетевое экранирование, предъявляются следующие требования:

- обеспечение безопасности внутренней защищаемой сети и полный контроль над внешними подключениями и сеансами связи;
- обладать мощными и гибкими средствами управления политикой безопасности организации;
- незаметная работа для пользователей локальной сети при выполнении ими легальных операций;
- обладать свойствами самозащиты от любых несанкционированных воздействий.

Если каналы связи выходят за пределы территории предприятия, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты.

В ходе своей деятельности типовому предприятию необходимо отправлять данные по открытым каналам связи в следующие организации:

- Пенсионный фонд Российской Федерации.
- Федеральная налоговая служба (ИФНС).
- Фонд Социального Страхования Российской Федерации.
- Сбербанк.
- Федеральное казначейство.
- Общероссийский Официальный Сайт (ООС) (Госзакупки).

Все организации требуют для передачи данных использовать различные сертифицированные средства криптографической защиты информации.

При проведении оценки актуальности угроз безопасности для типового предприятия должны быть выявлены следующие актуальные угрозы информационной безопасности, которые частично или полностью можно устранить за счет установки охранной сигнализации и сейфов для хранения документов и носителей информации:

- кража ПЭВМ;
- кража носителей информации;
- кража, модификация, уничтожение информации;
- вывод из строя узлов ПЭВМ, каналов связи;
- несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ;
- несанкционированное отключение средств защиты.

Организационно-правовые методы защиты информации

Создавая комплексную систему информационной безопасности, необходимо четко понимать, что без правового обеспечения защиты информации любые последующие претензии со стороны организации к недобросовестному сотруднику, клиенту или должностному лицу окажутся беспочвенными. Таким образом, состав защищаемой информации в каждой организации должен быть четко определен и задокументирован.

Организационные меры по защите конфиденциальной информации включают в себя:

1. Разработка организационно-распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты конфиденциальной информации:

- положение об обработке конфиденциальной информации;
- положение по защите конфиденциальной информации;
- инструкция оператора и администратора безопасности по защите конфиденциальной информации и др.

2. Разработка перечня мероприятий по защите конфиденциальной информации:

- определение круга лиц, допущенных к обработке конфиденциальной информации;
- организация доступа в помещения, где осуществляется обработка конфиденциальной информации;
- разработка должностных инструкций о порядке работы с конфиденциальной информацией;
- установление персональной ответственности за нарушения правил обработки конфиденциальной информации и др.

В ходе создания комплексной системы защиты конфиденциальной информации для типового предприятия, должен быть разработан комплект организационно-правовых документов, представленных в таблице 2.

Таблица 2

Организационно-правовые документы для предприятия

Название
О закреплении объектов информатизации за ответственными лицами
О назначении ответственных в подразделениях организации за эксплуатацию средств защиты информации
О порядке использования в помещениях организации радиотелефонов, сотовых и пейджинговых устройств при проведении конфиденциальных совещаний
О формировании системы обеспечения безопасности информации в организации
О порядке хранения конфиденциальной информации на электронных носителях
О назначении ответственных за обработку конфиденциальной информации
Приказ о проведении внутренней проверки
Приказ об электронном журнале обращений пользователей информационной системы к конфиденциальной информации
Приказ об утверждении положения об обработке и защите конфиденциальной информации работников
О порядке хранения конфиденциальной информации на электронных носителях
Инструкция по организации антивирусной защиты

Название
Инструкция по организации парольной защиты
Должностная инструкция администратора информационной системы
Инструкция пользователя информационной системы
Инструкция пользователя по обеспечению безопасности обработки конфиденциальной информации, при возникновении внештатных ситуаций
Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных средств защиты информации
Акт приема зачета по знанию нормативной базы
Акт классификации информационной системы предприятия
О порядке обработки конфиденциальной информации без использования средств автоматизации
О разграничении прав доступа к обрабатываемой конфиденциальной информации
Ведомость приема зачета по знанию нормативной базы
Места хранения конфиденциальной информации (материальных носителей)
Список сотрудников, ознакомленных с документами по работе с конфиденциальной информацией
Концепция информационной безопасности
Должностная инструкция администратора информационной системы
Перечень защищаемых объектов информатизации
Перечень информационных ресурсов конфиденциального характера
Перечень информационных ресурсов подлежащих учету и регистрации
План внутренних проверок
План мероприятий по обеспечению защиты конфиденциальной информации
Модель угроз безопасности конфиденциальной информации
Отчет о результатах проведения внутренней проверки
Перечень конфиденциальной информации, подлежащей защите
Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации
Журнал учета мероприятия по контролю
Журнал учета обращений субъектов конфиденциальной информации о выполнении их законных прав
Политика информационной безопасности

Заключение

Проведенный анализ методов и способов защиты информации на предприятии от несанкционированного доступа позволяет сделать вывод, что недостаточно просто закупить, установить и настроить средства защиты, но необходимо, с точки зрения законодательства и руководящих документов служб, осуществляющих надзор за обработкой конфиденциальной информацией, разработать документацию предприятия в области обеспечения информационной безопасности.

ЛИТЕРАТУРА

1. **Норткат, С.** Обнаружение нарушений безопасности в сетях, 3-е издание / С. Норткат, Д. Новак; пер. с англ. В.С. Иващенко. – М.: Вильямс, 2003. – 448 с.
2. **Козиол, Дж.** Искусство взлома и защиты систем / Дж. Козиол, Д. Личфилд, Д. Эйтел, К. Энли и др.; пер. с англ. Е. Матвеева. – СПб.: Питер, 2006. – 416 с.
3. **Андрончик, А.Н.** Защита информации в компьютерных сетях. Практический курс: учеб. пособие / А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков, М.Ю. Щербаков; под ред. Н.И. Синадского. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.
4. **Малюк, А.А.** Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов / А.А. Малюк. – М.: Горячая линия-Телеком, 2004. – 280 с.
5. **Варлатая, С.К.** Программно-аппаратная защита информации: учеб. пособие / С.К. Варлатая, М.В. Шаханова. – Владивосток: ДВГТУ, 2007. – 318 с.
6. **Соколов, А.В.** Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК Пресс, 2002. – 656 с.

Ivan Treschev
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: kalkt@yandex.ru

Protection from unauthorized access to information on the company

Abstract. This paper analyzes the organizational and administrative documents, which must be in the company in order to protect against unauthorized access to confidential information processed in information systems. The analysis of certified software and hardware protection.

Keywords: information security; security system; security threats.

REFERENCES

1. Nortkat, S. Obnaruzhenie narushenij bezopasnosti v setjah, 3-e izdanie / S. Nortkat, D. Novak; per. s angl. V.S. Ivashhenko. – M.: Vil'jams, 2003. – 448 s.
2. Koziol, Dzh. Iskusstvo vzloma i zashhity sistem / Dzh. Koziol, D. Lichfild, D. Jejtel, K. Jenli i dr.; per. s angl. E. Matveeva. – SPb.: Piter, 2006. – 416 s.
3. Andronchik, A.N. Zashhita informacii v komp'juternyh setjah. Prakticheskij kurs: ucheb. posobie / A.N. Andronchik, V.V. Bogdanov, N.A. Domuhovskij, A.S. Kollerov, N.I. Sinadskij, D.A. Hor'kov, M.Ju. Shherbakov; pod red. N.I. Sinadskogo. – Ekaterinburg: UGTU-UPI, 2008. – 248 s.
4. Maljuk, A.A. Informacionnaja bezopasnost': konceptual'nye i metodologicheskie osnovy zashhity informacii: ucheb. posobie dlja vuzov / A.A. Maljuk. – M.: Gorjachaja linija-Telekom, 2004. – 280 s.
5. Varlataja, S.K. Programmno-apparatnaja zashhita informacii: ucheb. posobie / S.K. Varlataja, M.V. Shahanova. – Vladivostok: DVGTU, 2007. – 318 s.
6. Sokolov, A.V. Zashhita informacii v raspredelennyh korporativnyh setjah i sistemah / A.V. Sokolov, V.F. Shan'gin. – M.: DMK Press, 2002. – 656 s.