УДК 004.056

В.В. Федько, И.А. Ряснянская

Харьковский национальный экономический университет, Харьков

ЗАЩИТА ПРАВ СОТРУДНИКОВ НА ПРЕДПРИЯТИИ ОТ РАЗГЛАШЕНИЯ ЛИЧНОЙ (КОНФИДЕНЦИАЛЬНОЙ) ИНФОРМАЦИИ В ПРОЦЕССЕ АТТЕСТАЦИИ

В данной статье рассматриваются проблемы нарушения прав человека, а именно разглашения личной информации о сотруднике на предприятии и за его пределами. Приведены основные статьи по защите прав человека в случае возникновения этой проблемы, а также статьи из законодательства касательно хищения информации. На примере программного модуля «Аттестация персонала» рассмотрены методы борьбы с несанкционированным доступом, а также средства обеспечения защиты информации.

Ключевые слова: *конфиденциальная информация, несанкционированный доступ, разглашение информации, распространение информации, права человека.*

Введение

Масштабы применения и приложения информационных технологий стали таковы, что наряду с проблемами производительности, надежности и устойчивости функционирования информационных систем (ИС), остро встает проблема защиты циркулирующей в системах информации от несанкционированного доступа [3].

Аттестация персонала является процессом, который подвергается риску утечки информации. Разглашение конфиденциальной информации, такой как результаты аттестации, преследуется законом Украины. Во Всеобщей декларации прав человека имеются следующие статьи:

Статья 8. Каждый человек имеет право на эффективное восстановление в правах компетентными национальными судами в случаях нарушения его основных прав, предоставленных ему конституцией или законом.

Статья 12. Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств [2].

К конфиденциальной информации в аттестации относятся: личное дело сотрудника, результаты аттестации, аттестационный лист, характеристика сотрудника.

Разглашение этой информации носит преступный характер, поскольку все эти данные можно использовать для унижения достоинства сотрудника, а также для использования готовых ответов и вопросов в личных целях, если сотрудник работает на этом же предприятии.

Основной материал

Автоматизация аттестации персонала на предприятии представляет собой электронный документооборот, начиная составлением приказа на проведение аттестации и заканчивая отчетностью по ней. Документы имеют как электронный вариант, так и бумажный.

Раньше главная проблема состояла в краже печатных документов и разглашении информации сотрудниками, что могло быть достаточно легко выявлено. В наши дни широко распространено незаконное оперирование электронными документами в компьютерных базах данных (БД), копирование электронной информации без фактической кражи носителя информации. Обнаружить такую кражу крайне сложно.

Предполагается, что защита информации осуществляется прежде всего от несанкционированного доступа к ней постороннего лица, который в результате этого доступа имеет возможность похитить информацию, уничтожить носитель, фальсифицировать сведения, произвести подмену документов или совершить иные злоумышленные действия [4].

Согласно закону Украины «О защите информации в автоматизированных системах» статья 17 «Ответственность за нарушение порядка и правил защиты информации» [1]:

Лица, виновные в нарушении порядка и правил защиты обработанной в автоматизированной системе информации, несут дисциплинарную, криминальную или материальную ответственность согласно действующего законодательства Украины.

Основными условиями утечки информации на предприятии являются:

неэффективная система защиты информации или отсутствие этой системы, что образует высокую степень уязвимости информации;

непрофессионально организованная технология обработки и хранения информации;

отсутствие системной аналитической и контрольной работы по выявлению и изучению угроз,

каналов и степени риска нарушений безопасности информационных ресурсов;

отсутствие контроля со стороны руководства фирмы за соблюдением персоналом требований нормативных документов по работе с информационными ресурсами ограниченного доступа;

неупорядоченный подбор персонала и текучесть кадров, сложный психологический климат в коллективе;

бесконтрольное посещение помещений фирмы посторонними лицами [4].

Существуют методы, которые позволяют несанкционировано вмешаться в работу системы:

запуск исполняемого кода;

осуществление операций чтения/записи файловых или других объектов;

обход установленных разграничений прав доступа;

троянские программы и др.

Для предотвращения этих угроз на предприятии необходимо иметь систему, которая устойчива к взлому, тем самым обеспечивая защиту информации.

На практике сегодня существует два подхода к обеспечению компьютерной безопасности:

использование только встроенных в операционную систему (ОС) и приложения средств защиты;

применение наряду со встроенными, дополнительных механизмов защиты – программных либо программно-аппаратных комплексов, устанавливаемых на защищаемые объекты [3].

Надежная система отвечает набору требований:

1. Идентификация и проверка подлинности субъектов доступа при входе в систему.

2. Идентификация терминалов, компьютеров, узлов компьютерной сети, каналов связи, внешних устройств по их логическим адресам (номерам).

3. Идентифицировать по именам программы, томов, каталогов, файлов, записей.

4. Контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа [3].

В работе рассмотрены возможные скрытые угрозы по утечке конфиденциальной информации в процессе проведения аттестации на небольшом предприятии с кадровым составом не более 30 сотрудников и соответствующие средства защиты информации.

Для компьютерной поддержки аттестации разработан программный модуль «Аттестация персонала». Он состоит из трех приложений: «Аттестация. Управление»; «Аттестация. Тест»; «Аттестация. Комиссия».

Они взаимодействуют через общую базу данных. Приложения имеют следующее назначение:

«Аттестация. Управление» – используется сотрудниками отдела кадров, непосредственно, ответственных за проведение аттестации. Это основное приложение, в нем формируются все документы, связанные с аттестацией: приказ о проведении аттестации, аттестационный лист, характеристика по сотруднику, отчет о проведении аттестации и др. Приложение обеспечивает доступ к личным данным по каждому сотруднику на предприятии. Возможность отслеживания прошедших аттестаций, их результаты и формирования отчетов по интересующим данным.

«Аттестация. Тест» – обеспечивает проведение аттестации для каждого сотрудника в индивидуальном порядке. Вопросы формируются в зависимости от занимаемой должности, а также от компетенции сотрудника. После того, как сотрудник ответит на набор вопросов, он получит результат на экране монитора, т. е. может сам оценить свои знания. Когда сотрудник узнает результат, данное приложение становится недоступным. Тестирование можно пройти только один раз в рамках одной аттестации.

«Аттестация. Комиссия» – приложение для аттестационной комиссии, т.к. на сегодняшний день отказаться от участия человека в компьютеризированном процессе крайне сложно. Оно основывается на результатах аттестуемых сотрудников, чтобы каждый член комиссии смог оценить полученный результат по оценочной шкале. Что станет итоговым результатом аттестации, т.е. результат за тестовые задания плюс оценка комиссии.

Обеспечение безопасности программного модуля достигается реализацией таких методов защиты данных, как парольная защита, разграничение прав доступа, а также контроль целостности данных.

Использование паролей длиной не менее 8 символов, которые хранятся на защищаемом объекте, обеспечивают защиту, однако этого не достаточно. С целью повышения уровня безопасности, для хранения пароля используется необратимое преобразование (хеш-функция), она позволяет создавать некий образ пароля – прямое преобразование. Этот образ соответствует паролю, но не позволяет осуществить обратное преобразование – из образа восстановить пароль. Для реализации необратимого преобразования используется алгоритм хеширования MD5 [3].

Рассмотрим угрозы преодоления парольной защиты.

Наиболее очевидными явными угрозами являются физические – хищение носителя, а также визуальный съем пароля при вводе. Кроме того, при использовании длинных сложных паролей пользователи подчас записывают свой пароль, что также является объектом хищения.

К техническим явным угрозам можно отнести подбор пароля, как автоматизированный, так и автоматический.

Наиболее опасными являются скрытые угрозы:

технический съем пароля при вводе;

модификация механизма парольной защиты;

модификация учетных данных на защищаемом объекте.

Отсюда следует, каким бы ни был механизм парольной защиты, он сам по себе в отдельности, без применения иных механизмов защиты, не может обеспечить высокий уровень безопасности защищаемого объекта.

Поэтому в программном модуле используются способы усиления парольной защиты за счет усовершенствования механизма ввода пароля.

На ввод пароля с клавиатуры используются такие ограничения:

на число неверно введенных значений пароля;

на возможность задания простых паролей;

на периодичность смены пароля пользователем.

Если количество неверно введенных значений пароля превосходит норму, то система блокирует доступ к системе.

Контроль целостности данных осуществляется путем установки системы, которая отслеживает все изменения с данными, а также производит резервное копирование.

При необходимости всю утерянную информацию возможно восстановить. Также можно просмотреть отчет об интересующей деятельности с тем или иным документом в программном модуле.

К задаче контроля целостности необходимо подходить с двух позиций. Во-первых, необходимо дать ответ на вопрос, с какой целью реализуется контроль целостности. Дело в том, что при корректной реализации разграничительной политики доступа к ресурсам их целостность не может быть несанкционировано нарушена. Отсюда напрашивается вывод, что целостность ресурсов следует контролировать в том случае, когда невозможно осуществить корректное разграничение доступа (например, запуск приложения с внешнего накопителя – для внешних накопителей замкнутость программной среды уже не реализовать), либо в предположении, что разграничительная политика может быть преодолена злоумышленником. Система защиты информации (СЗИ) от несанкционированного доступа, которая могла бы обеспечивать 100% защиту, построить невозможно даже теоретически. Необходимо понимать, что контроль целостности – это весьма ресурсоемкий механизм, поэтому на практике допустим контроль (а тем более с высокой интенсивностью, в противном случае, данный контроль не имеет смысла) лишь весьма ограниченных по объему объектов [5].

Учитывая многообразие потенциальных угроз информации на предприятии, сложность его структуры, а также участие человека в технологическом процессе обработки информации, цели защиты информации могут быть достигнуты путем создания СЗИ на основе комплексного подхода (рис. 1) [6].

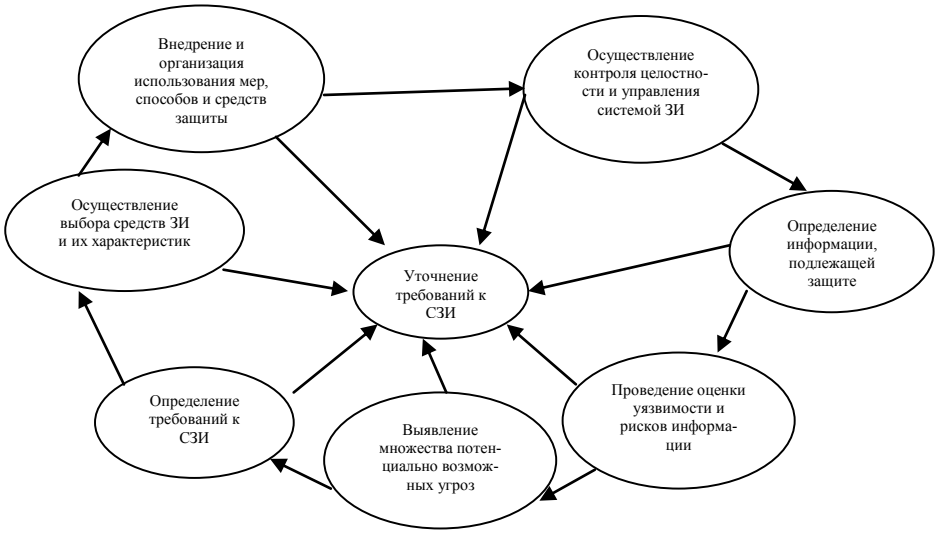

Рис. 1. Непрерывный цикл создания СЗИ

Специфика аттестации состоит в том, что она проводится через определенные предприятием промежутки времени. Поэтому приложение используется только тогда, когда необходимо провести аттестацию. Использование перечисленных средств защиты информации являются вполне подходящими. Сотрудники, которые работает с программными модулями «Аттестация. Тест» и «Аттестация. Комиссия», не сможет зайти в систему, если в основном модуле «Аттестация. Управление» нет приказа на проведение аттестации, а соответственно и сформированных паролей для каждого сотрудника тоже

нет. Это уже сужает круг потенциальных злоумышленников.

Механизмы идентификации и аутентификации предусматривают противодействие всем потенциальным злоумышленникам, т.е. как сторонним по отношению к системе, так и санкционированным, зарегистрированным в ней.

Защита информации от стороннего сотрудника достигается гораздо проще, для этого используется парольная защита. Основной угрозой служат преднамеренные или неумышленные действия санкционированного пользователя, который обладает возможностью осуществления скрытой атаки на защищаемый ресурс [3].

Даже если система защиты на данном этапе развития предприятия удовлетворяет всем вышеперечисленным требованиям, то в дальнейшем ее усовершенствование позволит защитить данные от несанкционированного доступа, который со временем модифицируется и принимает более новые формы.

Выводы

Принципы системного подхода при проектировании системы защиты должны отвечать таким требованиям:

любой механизм защиты должен проектироваться с учетом его влияния на безопасность системы в целом и с учетом функций защиты, реализуемых другими механизмами, т. е. учитываться влияние подсистемы на систему в целом;

проектирование системы защиты – многокритериальная задача. Поэтому при разработке механизма защиты должен учитываться не только обеспечиваемый им уровень безопасности, но и его влияние на производительность защищаемого объекта [3].

Для обеспечения защиты конфиденциальных данных в процессе аттестации целесообразно использовать следующие средства:

разбиение основного модуля на составные приложения для ограничения доступа сторонних пользователей;

составление матрицы полномочий сотрудников для разграничения прав доступа к приложениям;

использование паролей с дополнительными механизмами защиты;

контроль целостности данных путем регистрации деятельности сотрудников, а также резервного копирования данных.

Список литературы

1. Закон України «Про захист інформації в автоматизованих системах» від 5 липня 1994 року.

2. Всеобщая декларация прав человека (рос/ укр). Принята и провозглашена в резолюции 217А (III) Генеральной Ассамблеи от 10 декабря 1948 года.

3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. / А.Ю. Щеглов – СПб.: Наука и Техника, 2004. – 384 с.

4. Корнеев И.К. Защита информации в офисе: учебник / И.К. Корнеев, Е.А. Степанов. – М. : ТК Велби, Проспект, 2008. – 336 с.

5. Контроль целостности и аудит событий. [Электронный ресурс]. – Режим доступа к ресурсу: http://sio.su/down_asec_451_def.aspx.

6. Гришина Н.В. Организация комплексной системы защиты информации. / Н.В. Гришина. – М.: Гелиос АРВ, 2007. – 256 с.

Поступила в редколлегию 16.04.2011

Рецензент: д-р техн. наук, проф. Е.П. Путятин, Харьковский национальный университет радиоэлектроники, Харьков.

ЗАХИСТ ПРАВ ПРАЦІВНИКІВ НА ПІДПРИЄМСТВІ ВІД РОЗГОЛОШЕННЯ ОСОБИСТОЇ (КОНФІДЕНЦІЙНОЇ) ІНФОРМАЦІЇ В ПРОЦЕСІ АТЕСТАЦІЇ

В.В. Федько, І.О Ряснянська

У даній статті розглядаються проблеми порушення прав людини, а саме розголошення особистої інформації про співробітника на підприємстві і за його межами. Наведено основні статті по захисту прав людини у разі виникнення цієї проблеми, а також статті із законодавства щодо розкрадання інформації. На прикладі програмного модуля «Атестація персоналу» розглянуті методи боротьби з несанкціонованим доступом, а також засоби забезпечення захисту інформації.

***Ключові слова**: конфіденційна інформація, несанкціонований доступ, розголошення інформації, поширення інформації, права людини.*

PROTECTING THE RIGHTS OF EMPLOYEES IN THE COMPANY FROM DIVULGING PERSONAL (CONFIDENTIAL) INFORMATION IN THE QUALIFICATION PROCESS

V.V. Fedko, I.A. Ryasnyanskaya

This article discusses the problems of human rights breaches, namely the disclosure of personal information about an employee in the enterprise and beyond. Consider the main articles for the protection human rights, the articles from the legislation about information theft. Consider methods of fight with unauthorized access, a means of ensuring information security on the example software module "Certification of personnel".

***Keywords**: confidential information, unauthorized access, disclosure, dissemination, human rights.*