Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. Том 1 (67). 2015 г. № 1. С. 27–31.

УДК 004.056.5

ПРОБЛЕМАТИКА КОМПЛЕКСНОЙ ОЦЕНКИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Бойченко О. В., Белименко Б. В.

Крымский федеральный университет имени В. И. Вернадского, Симферополь, Российская Федерация
E-mail: bolek61@mail.ru

В статье рассматриваются современные проблемы анализа и оценки уровня защиты информационных ресурсов предприятия. Проанализированы наиболее важные факторы выбора адекватных методов защиты информации для принятия оптимального решения по повышению уровня информационной безопасности автоматизированной системы управления предприятием. Предложены ключевые механизмы комплексной оценки системы информационной безопасности предприятия.
Ключевые слова: информационные ресурсы, методы защиты информации**,** комплексная система оценки, матрица доступа, конфиденциальные данные.

ВВЕДЕНИЕ

Информационные технологии в настоящее время активно внедряются во все сферы деятельности. Быстро развивающийся рынок электронных информационных продуктов и услуг предлагает большое количество отечественных и зарубежных экономических информационных систем различного назначения. Сегодня информационные ресурсы играют важную роль в деле повышения конкурентоспособности, инвестиционной привлекательности и капитализации компании. В связи с этим возрастает угроза нежелательного использования ресурсов, хранящих данные, прямо влияющие на жизнедеятельность и развитие компании.

Внедрение во все сферы управленческой деятельности современных информационных технологий, обеспечивающих автоматизацию документооборота, выдвигает на первый план задачи защиты информационных ресурсов от воздействия угроз. Такие угрозы обусловлены как внутренними, так и внешними факторами среды современных информационно-коммуникационных систем. Их слабая защищенность при многих обстоятельствах может стать причиной экономических потерь.

В интересах государства в информационной сфере – развивать информационные технологии, процессы, методы поиска, сбора, хранения, обработки, распространения и предоставления информации. Одновременно с развитием растут риски угроз безопасности информационных ресурсов. В свете того, что российская экономика все больше интегрируется в мировую, необходимо соблюдение международных требований конфиденциальности, защиты информационных ресурсов [1].

Для обеспечения безопасности необходимо решить задачу обеспечения конфиденциальности, целостности и доступности, что требует создания соответствующего инструментария для их оценки. Предпринимаемые меры защиты должны быть адекватны вероятности осуществления определенного типа угрозы и

потенциальному ущербу, который может быть нанесен в том случае, если угроза осуществится [2].

Цель исследования состоит в анализе проблематики анализа и оценки уровня защиты информационных ресурсов, разрешений доступа и использования конфиденциальной информации на предприятии для обеспечения необходимого уровня безопасности корпоративных данных, необходимых для принятия управленческого решения.

ОСНОВНОЙ МАТЕРИАЛ

В современных корпоративных реалиях большое количество важной для организации информации хранится в виде так называемых неструктурированных или полуструктурированных данных в виде отдельных файлов и папок на файловых хранилищах, коллекциях сайтов SharePoint, архивов электронной почты на серверах Exchange и т. д. Объем роста таких данных составляет, в среднем, около 30–50% в год.

Причем такими темпами происходит не только количественный рост объемов, потребляемых для хранений байт, но и качественное увеличение важных или даже жизненном необходимых для компании данных, «размазанных» по одному или нескольким (иногда 20–30) файловым серверам с разными операционными системами, идеологиями хранения и обработки информации (Exchange, SharePoint, Windows, SAN/NAS).

Анализ сведений об основных причинах утечки данных позволяет выделить следующие направления уязвимости информационных ресурсов предприятия:

- уязвимости, связанные со служебной необходимостью доступа к данным клиентов, личным делам сотрудников, финансовым отчетам и другим конфиденциальным документам, – 76%;
- уязвимости, связанные с возможностью получения доступа к «множеству данных», не связанных со служебной деятельностью, – 38%;
- уязвимости, связанные с организационными просчетами конечных пользователей по защите доступных им корпоративных данных, – 47%;
- уязвимости, связанные с возможностью переноса рабочих документов на персональные устройства, – 76%;
- уязвимости, связанные с низким уровнем контроля потерь документов, файлов или почтовых сообщений, – 49%;
- уязвимости, связанные с неосведомленностью бизнес-пользователей организации о случаях потерь или кражи корпоративных данных, – 44%.

Указанные обстоятельства порождают ряд проблем по обеспечению безопасности корпоративных данных, оптимизации их хранения, а также управлению и взаимодействию сотрудников организации по обеспечению необходимого уровня защиты информационных ресурсов предприятия.

Традиционно к решению указанных задач привлекаются сотрудники IT-подразделения для системного администрирования компьютерных ресурсов компании, а также сотрудники управления информационной безопасности,

заинтересованные в минимизации рисков, связанных с утечкой или порчей или инымвредным для компании использованием конфиденциальной информации [3].

Также во многих организациях, помимо технических специалистов и специалистов информационной безопасности, предназначение и важность использования специфической информации лучше всего представляют сотрудники профильных для компании подразделений: юристы, бухгалтеры, сотрудники отделов продаж и т. п. Вовлечение таких сотрудников в качестве «владельцев данных» привносит ценный вклад в решение задач по обеспечению безопасности данных, актуализации важной информации и т.п. [4].

Совокупность действий по решению обозначенных проблем может быть реализована в организации комплексом мер в составе разработки соответствующих регламентов и внутренних политик, обучением технического персонала и внедрением технических средств, обеспечивающих реализацию этих мер на предприятии.

Анализ функционирования современных распределенных информационных систем управления позволяет выделить следующие компоненты комплекса мер информационной безопасности корпоративных данных:

1. Правила доступа являются отправной точкой в выстраивании политик безопасности данных, что обеспечивает предоставление исчерпывающей информации о субъектах доступа, их прав на конкретный ресурс отдела, а также анализ возможностей доступа через глобальные группы и т. д. Это обеспечивает значительное снижение рисков утечки и неправомерного использования информационных ресурсов корпорации;

2. Классификация информационных ресурсов позволяет произвести необходимое разделение данных по приоритетам, что позволяет создать условия для обеспечения целостности и конфиденциальности корпоративных данных;

3. Маркировка «владельцев данных» в соответствие с иерархией распределения прав доступа к конкретным ресурсам и каталогам создает условия для организации функционирования кардинально нового эффективного инструмента, позволяющего определить права доступа к конкретной папке до минимально необходимого уровня;

4. Мониторинг и аудит действий текущей активности пользователей на файловых хранилищах позволяет осуществить общий мониторинг файлового ресурса. Важным также является возможность эффективного мониторинга обращений к персональным данным сотрудников, а также оперативного анализа инцидентов, связанных с удалением и копированием информации конкретными пользователями и т. д.;

5. Оперативное оповещение о происходящих событиях на файловой системе автоматизированной системы управления создает условия для оперативного выявления фактов несанкционированного влияния на автоматизированную информационную систему (АИС), что позволяет пресекать подобные инциденты и предотвращать факты нецелевого использования информации на начальном этапе, существенно снижая уровень возможных вредных последствий.

6. Использование журнала событий обеспечивает применение нового подхода к анализу и оценке целостности файловой системы АИС, что позволяет устанавливать действия пользователей по работе с файлами, особенно те, которые выходят за рамки установленного регламента обработки корпоративных информационных ресурсов.

7. Гибкое использование коммуникационной составляющей современных информационных систем управления корпорацией, характеризующихся высоким уровнем интегрирования и распределения данных, необходимых для принятия адекватного управленческого решения и получения максимальной прибыли производства. Как следствие, для обеспечения высокой организации АИС требуется необходимая коммуникационная составляющая, основанная на использовании интернет.

При этом следует выделить особый класс взаимодействий, предназначенный для осуществления передачи конфиденциальной информации (личные данные, секретные сообщения) или команд, выполнение которых должно быть кем-то однозначно подтверждено (например, перевод денег или публикация сообщения от чьего-то имени).

В такой ситуации возникает проблема необходимости надежной защиты подобных сервисов от злоумышленников, связанная с довольно невысокой степенью защищенности приложений.

Кроме того, проблема усугубляется тем, что многие представители электронного бизнеса разрабатывают протоколы, которые, будучи реализованными в конечных сервисах, могут создать серьезные уязвимости, если использовать их без должного понимания.

При этом для осуществления необходимой производственной коммуникации, необходимо соблюдение правил безопасного взаимодействия, основанных на проведении аутентификации серверов пользователей, обеспечении целостность пакетов данных, проходящих по каналу связи, а также обеспечении конфиденциальности взаимодействия с применением криптографических методов защиты информации.

ВЫВОДЫ

В результате проведенного анализа были выдвинуты основные меры и рекомендации к безопасному использованию и хранению информационных ресурсов предприятия.

Необходимо отметить, что указанные рекомендации являются отправной точкой для выстраивания адекватной корпоративной политики информационной безопасности хранения данных.

Использование разработанного комплекса мер создает условия для решения первостепенных задач безопасности корпоративных данных, таких как:

- повышение уровня безопасности имеющейся информации;
- повышение эффективности использования данных в принятии управленческих решений;

- сокращение времени администрирования и обеспечение безопасности файловых хранилищ;
- обеспечение четкого понимания возможных рисков, связанных с нецелевым использованием данных и способами минимизации этих рисков.

Список литературы

1. Крошилин С.В., Медведева Е.И. Информационные технологии и системы в экономике: учебное пособие. М.: ИПКИР, 2008. 485 с.
2. Майкл Ховард, Дэвид Лебланк. «Защищенный код» Microsoft Press. М., 2012. 251 с.
3. Стоянова О.В., Зайцев О.В. Метод дерева целей для оценки эффективности использования информационных ресурсов // Программные продукты и системы. 2009. 215 с.
4. Юрков, Н. К. К проблеме обеспечения глобальной безопасности // Надежность и качество: тр. Междунар. симп.: в 2 т. / под ред. Н. К. Юркова. Пенза: Изд-во ПГУ, 2012. Т. 1. 194 с.

Статья поступила в редакцию 26.10.2015