УДК 004.056

РАЗРАБОТКА ИТ-СТРАТЕГИИ И АВТОМАТИЗАЦИЯ ПРОЦЕССОВ УСИЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ПРОИЗВОДСТВЕННО-ЗАГОТОВИТЕЛЬНОГО ХОЛДИНГА

DEVELOPMENT OF IT-STRATEGY AND AUTOMATION OF THE PROCESSES OF STRENGTHENING THE PROTECTION OF DATAWARE OF AN INDUSTRIAL AND STORAGE HOLDING COMPANY

С.А. ПАНКРАТОВ, А.В. ФИРСОВ
S.A. PANKRATOV, A.V. FIRSOV

(Московский государственный текстильный университет им. А.Н.Косыгина)
(Moscow State Textile University "A.N. Kosygin")
E-mail: StanAPankratov@gmail.com, Firsov_A_V@mail.ru

В работе описан один из основных медов разработки ИТ-стратегии, использующий компонентную модель бизнеса. Исследования выполнены на базе производственно-заготовительного холдинга по заготовке, обработке и сбыту вторсырья. Проведено исследование и сравнение способов защиты электронной информации, в том числе с использованием графических средств. В результате оценки стойкости парольной защиты существующих способов аутентификации разработана программа графической аутентификации, которая является более стойкой к взлому пароля.

The article describes one of the basic methods of IT-strategy development using a component business model. The research has been carried out on the basis of the industrial and storage holding company, engaged in storage, processing and sale of secondary raw materials. Research and comparison of the ways of electronic information protection, including graphic means.

Ключевые слова: анализ, автоматизация, ИТ-стратегия, компонентная модель, бизнес, производство, аутентификация, защита, графическая аутентификация, пароль, информационное обеспечение.

Keywords: analysis, automation, IT-strategy, component model, business, manufacturing, authentication, security, graphics authentication, password, information provision.

Исследования выполнены на базе производственно-заготовительного предприятия (ПЗП) по заготовке, первичной обработке и сбыту вторичного сырья (текстильных отходов). ПЗП состоит из производственного, транспортного и головного подразделений, каждое из которых является отдельным юридическим лицом и находится не в одном здании, офисе, а на удаленном друг от друга расстоянии. Это управляющая компания, ПЗП №1 и ПЗП №2 вместе с транспортной компанией. Между этими отделами происходит ежедневный обмен информацией:

– финансовая информация (цены на покупку и продажу текстильного вторсырья, бухгалтерия и т.п.);

– объемы заготовки и отгрузки текстильного вторсырья (аналитика, логистика);

– информация о собственном автопарке (логистика);

– информация о поставщиках (клиентах);

– и т.д.

Как и на любом другом действующем предприятии, в холдинге имеется информация, которая не должна выходить за его

"стены". Но, как показывает далее первичный опрос, большинство персонала даже и не задумываются о том, что кража или потеря вышеперечисленной информации может привести к остановке производства или даже банкротству компании.

Решение проблем, возникающих в существующей системе безопасности информационного обеспечения предприятия, можно представить в виде комплекса методов защиты корпоративной информации, разбитых на следующие уровни:

– социальный уровень,
– физический уровень,
– технический уровень,
– программный уровень.

Социальный уровень. Набор корпоративных правил в компании относительно информационной безопасности. Например, запрет на самовольный внос и вынос каких-либо носителей информации (flash-носители, жесткие диски, компьютеры, ноутбуки). Ряд мероприятий (конференции, совещания), посвященных безопасности информационного обеспечения в компании.

Совещания и переговоры, в процессе которых могут обсуждаться сведения, составляющие тайну фирмы или ее партнеров, именуются обычно конфиденциальными. Порядок проведения подобных совещаний и переговоров регламентируется специальными требованиями, обеспечивающими безопасность ценной, в том числе конфиденциальной, информации (далее – ценной информации), которая в процессе этих мероприятий распространяется в санкционированном (разрешенном) режиме. Основной угрозой ценной информации является разглашение большего объема сведений о новой идее, продукции или технологии, чем это необходимо [1].

Причины, по которым информация может разглашаться на конфиденциальных совещаниях или переговорах, общеизвестны: слабое знание сотрудниками состава ценной информации и требований по ее защите, умышленное невыполнение этих требований, провоцированные и непровоцированные ошибки сотрудников, отсутствие контроля за изданием рекламной и рекламно-выставочной продукции и др. Оглашение ценной информации в санкционированном режиме должно быть оправдано деловой необходимостью и целесообразностью для конкретных условий и характера обсуждаемых вопросов.

Физический уровень. Исключение причинения вреда информации со стороны похищения и уничтожения информации. От похищения используются уничтожители информации с магнитных носителей (жестких дисков, HDD). В случае несанкционированного доступа или при попытке кражи устройства с информацией такой уничтожитель сработает и удалит всю информацию на носителе без возможности ее восстановления. От незапланированного физического уничтожения информации носители с ней помещаются в специальные хранилища, например, в серверные шкафы с замками, в специальные сейфы, или, как минимум, в хорошо запираемое помещение.

Технический уровень. Первое, что приходит в голову, это желание лишить сотрудника возможности вынести информацию из ИТ-системы техническими мерами. Вот пути, по которым информация может покинуть организацию [2]:

1) электронная почта;
2) Web-сайты (Web-почта, форумы и т.п.);
3) ПО для обмена мгновенными сообщениями;
4) сменные носители;
5) распечатки;
6) сети Wi-Fi, Bluetouth;
7) модемы (сотовые и обычные);
8) снимки экрана фотоаппаратом или камерой сотового телефона;

Из этого можно сделать следующий вывод: Каналы утечки характеризуются пропускной способностью. Если через 4 и 6-й каналы можно легко унести базу данных в несколько гигабайт, то для того, чтобы сделать это по 1 или 7-му каналу, потребуется уже много времени и усилий. А по 5 или 8-му каналам сделать это, вероятно, не удастся и вовсе. В то же время утечка персональных данных об отдельно взятом клиенте возможна по любому из этих каналов, точно так же, как и о маркетинговых планах компании. Для некото-

рых каналов есть возможность обеспечить довольно развитую политику безопасности. Например, для почты, доступа в Интернет и сменных носителей можно запретить передачу конфиденциальной информации. Дальше хуже. Печать, Wi-Fi, модемы можно или разрешить, или запретить. Фотоаппараты запретить крайне тяжело. Устное общение запретить нельзя. Более того, теоретически доказано, что если информационная система не замкнута, то сеть взаимодействует с внешним миром, существование скрытых каналов возможно. Вопрос может ставиться только о пропускной способности такого канала или о времени, которое потребуется, чтобы его построить.

Программный уровень. Защитить информацию не только от несанкционированного доступа к ней, но и от ошибок пользователей. Необходимо создать разграничение доступа к информации. Такое разграничение предоставляет аутентификация OS Windows во взаимодействии с аутентификацией БД. У каждого пользователя существует свое имя входа и пароль (представляют собой два текстовых поля) для получения доступа к личному рабочему месту [3]. А также использовать аутентификацию на уровне подключения к базам данных. Например, только весовщица на приемном пункте может добавить в базу заготовку вторсырья, так как данные поступают с весов. Ни менеджер, ни кассир, который выдает за привезенное вторсырье деньги, и даже не руководитель производственного участка не имеет права добавлять заготовку в ИС компании.

Но перед тем как принимать какие-либо меры по усилению защиты информации в холдинге, необходимо понимать:

– бизнес-процессы компаний по отдельности и холдинга в целом;

– внутренние и внешние потоки информации;

– текущее состояние бизнеса;

– цели и задачи бизнеса.

Если не ознакомиться с бизнесом, то можно необоснованными изменениями в ИТ-инфраструктуре компании помешать достижению ее целей. Для этого необходимо построить компонентную модель бизнеса.

Компонентная модель бизнеса для ИТ (Component Business Model for the Business of IT) позволяет представить организацию ИТ и суть деятельности подразделений ИТ-службы в виде набора основных компетенций и компонентов. Состав компонентов определен на основе лучшего мирового опыта для подразделений ИТ и предприятий, оказывающих услуги в области ИТ. Такой подход помогает идентифицировать возможности для улучшения и инноваций, в том числе провести укрупненный анализ ИТ-службы компании для принятия решений по внедрению процессов управления ИТ, а также организационным преобразования [4].

Одна из целей компонентного моделирования – обеспечить "модульность" представления компетенций бизнеса, повышая таким образом наглядность и управляемость. Компонентная модель представляет бизнес Компании в виде взаимодействующих специализированных наборов функций – бизнес-компонентов. На основании понимания бизнеса Компании, встреч с высшим руководством и руководителями подразделений, определяются "компетенции" бизнеса и формируется матрица, в которую заносятся текущие и планируемые бизнес-функции. Далее бизнес-функции группируются по компонентам на основании схожести характеристик рассматриваемых функций в области организационных и информационных технологий. Для этого нужно определить наборы функций, которые могут быть логически объединены в уникальные (в рамках создаваемой модели) бизнес-компоненты, а также понять информационное взаимодействие этих бизнес-компонентов. "Кандидатами" на объединение в бизнес-компоненты являются близкие по смыслу либо смежные функции, которые лежат в одной предметной области, используют общий пул информационных ресурсов и схожие технологии.

И только в последнюю очередь необходимо соотнести бизнес-компоненты с ИТ-сервисами и их функциями и выявить

сильные и слабые стороны в ИТ-инфраструктуре, например:

1. ActiveDirectory: инфраструктура;
2. Internet: синхронизация баз, поиск клиентов и поставщиков;
3. Электронная почта (аутсорсинг): большая часть электронной почты проходит через личные почтовые аккаунты (Google, Mail.ru, Yandex), а также существует почтовые аккаунты на аутсорсинге;
4. БД (Access): консолидированные данные по основной, коммерческой и финансовой деятельности;
5. 1С: Бухгалтерия и Кадры;
6. Microsoft Excel/ Word: БДДС, кадровый учет, отчетность;
7. АРМ Заготовка: сбор информации о заготовке;
8. АРМ Касса: финансовые проводки, отчеты;
9. АРМ Отгрузка: сбор информации по отгрузке;
10. Сайт компании: визитная карточка компании;
11. PGP: шифрование документов (при отправке по электронной почте);
12. Навигатор: отслеживание собственного транспорта и аналитика.

По результатам анализа функций производственно-заготовительного холдинга можно сделать следующие выводы.

1. Холдинг имеет сильную производственную часть (производство, складирование).
2. В холдинге все составляющие его компании имеют как свою собственную бухгалтерию, так и "общую".
3. Очень слабо технически развита ИТ-архитектура.
4. На низком уровне находится:

a. поиск клиентов и поставщиков,
b. логистика,
c. ИТ,
d. безопасность,
e. финансовая деятельность,
f. процесс бюджетирования.

Учитывая тот факт, что область действия, связанная с финансами, слабо развита на уровне ИТ, ее уровень необходимо повысить. Также необходимо создать развитую политику безопасности, как минимум, повысить уровень защиты информационного обеспечения на физическом и социальном уровнях.

ЛИТЕРАТУРА

1. Astera. Ударим графическим паролем против несанкционированного доступа. *Новости ИТ-бизнеса для Профессионалов.* [В Интернете] 1.10.2002 г. [http://www.astera.ru/news/?id=4467]
2. *Лобачев Е.* Защита информации от утечки из информационных систем // Infarmation Security/Информационная безопасность". – 2008, вып. 2.
3. Проблемы экономики и прогрессивные технологии в текстильной, легкой и полиграфической отраслях промышленности // Всероссийская науч.-техн. конф. (2009, Санкт-Петербург): Система графической аутентификации (тез. докл.). – СПб.: СПГУТД, 2009.
4. IBM. "Управление ИТ-услугами – подход IBM" [http://www.ibm.com/developerworks/ru/edu/dw-rt-modsoacase/section5.html]

Рекомендована кафедрой информационных технологий и компьютерного дизайна. Поступила 10.12.12.