НЕКОТОРЫЕ ПОДХОДЫ К СОЗДАНИЮ СИСТЕМ УПРАВЛЕНИЯ ЗНАНИЯМИ КОМПАНИЙ

Ольга Петрова, *"Compania Dekart" SRL (Республика Молдова)*

Успешность деятельности той или иной компании зависит от различных факторов. Одним из основных является уровень подготовки сотрудников, их квалификация и опыт.

1. Квалификация любого сотрудника нуждается в регулярном повышении
2. Опыт, который не передается другим, теряет половину своей ценности поскольку при этом не происходит накопления знания другими сотрудниками. Кроме того, увольнение сотрудника ведет к потери этого знания для компании, а переход сотрудника к конкурентам приведет к тому, что эти знания возможно будут работать на пользу других.

Цель работы – создать систему, позволяющую решить одновременно две задачи. Во-первых, создать сотрудникам эффективный доступ к информационным ресурсам компании. А во-вторых, обеспечить защиту интеллектуальной собственности компании, ее коммерческой тайны.

Противодействие угрозам, связанным с несанкционированным доступом к информации

1. Всю совокупность информации, накопленную компанией и постоянно обновляемую, следует классифицировать по различным признакам.
   a. По области применения – финансовая информация, технологические сведения, сведения о безопасности предприятия и т.п. (F_1, …, F_n).
   b. Внутри каждого тематического раздела информация должна быть разделена по уровню доступности – общедоступная (IR_f), доступная представителям отдельных групп (IR_g), доступная отдельным работникам (сотрудникам) (IR_p).
2. Штат (штатное расписание) компании разбивается на группы по профессиональной принадлежности и т.п.
3. Формируется матрица соответствия сотрудника и информационных ресурсов, доступных ему для чтения.
4. Создается LDAP-хранилище с персональными данными сотрудников, необходимыми для аутентификации в системе и персональный список доступных информационных источников – например, $P_1 \leftrightarrow\{(F_1, IR_f), (F_1, IR_p), (F_2, IR_f), (F_2, IR_g), \ldots, (F_n, IR_f), (F_n, IR_g)\}$, $P_2 \leftrightarrow$

{(F_1 , IR_f), (F_1, IR_g), (F_2, IR_f), (F_2, IR_p), …, (F_n, IR_p)}.

5. Доступ к информационной системе осуществляется только после аутентификации. При обращении к системе после аутентификации сотруднику получает доступ к информации (выдается список всех доступных источников или последний читаемый документ или список изменений в базе знаний или авто-напоминание).

6. Для доступа к особо важной информации вместо обычной аутентификации может применяться усиленная аутентификация.

Противодействие угрозам, связанным с нарушением процедуры размещения информации

1. Так же как и в предыдущем разделе, вся совокупность информации, необходимая компании, классифицируется по различным признакам F_1, …, F_n.
2. Внутри каждого тематического раздела информация разделяется по уровню ответственности – IW_g, когда право на запись есть у представителей отдельных групп, IW_p, когда право на запись есть только у отдельных работников.
3. Аутентификация для доступа к соответствующим разделам базы знаний осуществляется только после предъявления сертификата открытого ключа конкретного сотрудника.
4. Запись информации производится только при наличии цифровой подписи для подтверждения неизменности и неотрекаемости.

В целях реализации вышеперечисленных мер в компании должно быть предусмотрено использование инфраструктуры защиты информации на основе открытых ключей. Компания может развернуть собственный Центр сертификации открытых ключей либо воспользоваться услугами уже существующих Центров. Каждый из сотрудников генерирует свою пару ключей (секретный и открытый) и получает в Центре сертификации сертификат своего открытого ключа. Данный сертификат может быть использован для аутентификации сотрудника при обращении к базе знаний и для проверки цифровой подписи под размещенной там информацией.

Защита интеллектуальной собственности авторов

Для защиты прав авторов (их интеллектуальной собственности) предлагается один из разделов базы знаний превратить в интеллектуальный репозиторий. Авторы могут размещать свою информацию в данном разделе, заверяя ее своей цифровой подписью. Причем могут сохраняться не только законченные результаты, но и промежуточные, а также варианты решений. Законченные работы могут быть (и должны!) перенесены в основную базу знаний компании. При переносе документ подписывается (с помощью цифро-

вой подписи) лицом, осуществляющим данную операцию.

Обучающая составляющая системы знаний

Любое обращение к базе знаний компании должно быть запротоколировано в специальном файле – журнале операций. Данный модуль решал бы двуединую задачу – информационной безопасности компании и стал бы одной из компонент автоматизированного помощника самого сотрудника. На базе экспертных оценок подготовить авто-советника для сотрудников с целью повышения уровня их знаний.

Система контроля знаний

Выявление знания-незнания возможно за счет использования различных тестов. Тестирование может проходить как на добровольной основе, так и быть предусмотрено должностными обязанностями. Регулярность процедуры, размер теста и его уровень могут быть заданы исходя из сложности проблематики решаемых тем или иным специалистом вопросов, стажем работы в компании, ответственности при принятии решений, уровнем образования и т.д.:

1. ежемесячно, ежеквартально, раз в полгода, раз в год;
2. исходя из того, к каким разделам информационной базы сотрудник имеет доступ, составляется перечень тестов, их очередность, регулярность и уровень сложности;
3. если произошло обновление информационной базы, то можно после ознакомления с ней проводить мини-тест для определения степени усвоения материала;
4. при накоплении данных о том какие части информационных ресурсов посещаются сотрудником и с какой регулярностью программа-робот может предложить пройти тестирование по данным частям, а также по тем, которые посещаются гораздо реже либо не посещаются вовсе;
5. открытый вопрос о принудительности прохождения того или иного теста. Возможно имеет смысл применять тонкую интеллектуальную настройку системы управления знаниями. Например, не разрешать просматривать информацию из базы знаний, если не пройден тест, либо тест пройден с неудовлетворительным результатом. Второе предложение – автоматически открывать тот раздел базы знаний, по которому сотрудник не смог пройти тестирование.