КЛАССИФИЦИРУЕМ ПО КОНФИДЕНЦИАЛЬНОСТИ[1]

Алексей Пастоев, CISSP
apastoev@kerberus.ru

Сегодня как никогда ранее справедливо изречение: «Кто владеет информацией, тот владеет миром». Однако владеть информацией – это только полдела. Ее еще нужно уметь грамотно защищать. Однако трудно построить оборону, не определив стандарт классификации корпоративной информации по степени ее конфиденциальности.

Чтобы построить эффективную систему защиты информационных активов, любой компании необходимо определить степень ценности различных типов данных, знать, где они находятся, каким образом и кем обрабатываются и как уничтожаются в конце жизненного цикла. Без этих знаний будет сложно предотвратить утечки конфиденциальной информации и обосновать финансовые расходы на защиту информации.

Крупные отечественные компании обычно имеют внутренний приказ или распоряжение, описывающее типы информации, относящиеся к конфиденциальным данным или коммерческим сведениям. Однако определения типов информации, которые в них даются, зачастую весьма туманны (например «и другие сведения, составляющие коммерческую тайну»), кроме того, в них отсутствуют правила отнесения информации к той или иной степени конфиденциальности, а также правила обращения с теми или иными данными. Документ такого качества непригоден для использования на практике, особенно для защиты информации в электронной форме.

В крупных западных компаниях имеются хорошо проработанные корпоративные стандарты классификации информации, в которых перечисленные недостатки отсутствуют. Этому в значительной мере способствует более развитое законодательство в области защиты информации и привлечение сторонних консультантов, имеющих практический опыт в разработке документов по информационной безопасности.

Следует отметить, что в российском законодательстве имеется ряд законов, требующих от предприятия определенных усилий по защите своих информационных активов. В первую очередь следует отметить недавно принятый закон «О коммерческой тайне» от 29 июля 2004 года и Гражданский Кодекс РФ (статья 139 «Служебная и коммерческая тайна»). Данные законодательные акты ориентированы в основном на юридическую сторону вопроса защиты информации. Поэтому отечественному предприятию следует иметь внутренний стандарт, учитывающий специфику предприятия и определяющий правила классификации информации по приемлемой в практическом отношении «шкале конфиденциальности» и устанавливающий правила работы с классифицированной информацией, ее хранения и уничтожения. Этот стандарт определяет

[1] Статья опубликована в журнале «Директор ИС» №4, апрель 2005.

базовую политику в области информационной безопасности наравне с другими основополагающими корпоративными стандартами, такими как, например, стандарт по управлению рисками. Более развернутая шкала оценки степени конфиденциальности помогает оптимизировать финансовые затраты на защиту информационных активов.

НУЖЕН ДОКУМЕНТ

Как же правильно сформулировать стандарт классификации корпоративной информации по степени конфиденциальности для своей компании? На тему защиты информации и, в частности, ее классификации издано значительное количество книг и публикаций, но, к сожалению, русскоязычная литература по данной тематике, как правило, носит теоретический характер, а зарубежная содержит явный уклон в сторону обеспечения безопасности правительственных или военных информационных систем и базируется на иностранной законодательной базе.

Безусловно, теория важна. Однако, как применить ее на практике предприятию, действующему в условиях недостаточно развитой законодательной базой в этой сфере? Как определить, какая информация используется в компании, какую выбрать шкалу классификации и как правильно определить меры по защите данных?

Перед тем, как приступить к реализации каких-либо организационных и тем более технических мер в области информационной безопасности, необходимо разработать пригодный для практического использования документ, определяющий общие правила, но не технические детали в области классификации корпоративной информации по степени конфиденциальности. К сожалению, устоявшегося названия для этого документа в русском языке еще нет, в английском же его название звучит так: Data Classification Standard.

Этот документ должен быть формально утвержден высшим руководством компании, например, советом директоров или генеральным директором, в противном случае ваши дальнейшие усилия обречены на неудачу. Это не такая простая задача, как кажется на первый взгляд. В крупных компаниях (особенно холдингах) велика степень бюрократии, затрудняющая принятие подобного корпоративного стандарта. В таком случае потребуется ряд подготовительных действий, способствующих утверждению данного документа.

КЛЮЧЕВЫЕ ПУНКТЫ СТАНДАРТА

Что же должно быть в корпоративном стандарте классификации информации? Правильно составленный стандарт должен включать в себя следующие разделы:

- заявление руководства компании о важности защиты информационных активов;
- назначение стандарта классификации данных;
- принятые категории классифицированной информации;

- принципы отнесения информации к той или иной категории конфиденциальности;
- перечни используемых типов информации отнесенных к той или иной категории конфиденциальности;
- правила управления доступом и контроля доступа к классифицированным данным;
- правила применения методов защиты при передаче классифицированных данных;
- маркировка и методы хранения классифицированной информации;
- порядок уничтожения носителей с классифицированными данными;
- правила обращения с классифицированной информацией;
- срок следующего пересмотра стандарта.

Заявление руководства компании о важности защиты информационных активов. В данном пункте должна быть отражена позиция высшего руководства компании в отношении защиты информационных активов. Данным заявлением руководство компании выражает свою поддержку предпринимаемым мерам по защите информации.

Назначение стандарта классификации данных. Содержание этого раздела может быть примерно такое: «Информация является важным корпоративным ресурсом, который необходимо защищать вследствие его конфиденциальности и ценности для поддержки ключевых бизнес-процессов компании. Для обеспечения эффективной защиты значимых информационных ресурсов необходимо понимание того, что является значимой информацией, где находятся информационные ресурсы и каким образом осуществляется обработка информации. Это позволит с наименьшими затратами снизить риск разглашения конфиденциальной информации до приемлемого уровня». Целью данного стандарта также является определение правил обращения с классифицированной информацией компании.

Принятые степени классифицированной информации. Для практического применения стандарта в коммерческих компаниях имеет смысл использовать шкалу, состоящую из четырех степеней конфиденциальности: «публичная», «для внутреннего использования», «конфиденциальная» и «строго конфиденциальная». Более детализированная градация, например, «ограниченного распространения для бизнес-партнеров» (Business confidential) может привести к расплывчатости определений каждого класса данных, и должна использоваться только тогда, когда для этого есть объективные причины.

Принципы отнесения информации к той или иной категории конфиденциальности. В этом разделе следует дать четкие правила отнесения информации к той или иной категории конфиденциальности. Следует воздержаться от определений типа «и другие важные сведения».

Перечни используемых типов информации. В этом разделе указываются списки используемых типов информации, разбитых по категориям «строго конфиденциально», «конфиденциально», «для внутреннего использования» и «публичная информация». Также следует составить перечень типов используемой информации с указанием их степени конфиденциальности для каждого

крупного подразделения компании. В дальнейшем это облегчит ежегодное обновление стандарта.

Правила управления доступом и контроля доступа к классифицированным данным. Этот раздел должен определять принципы управления доступом к информации каждой степени конфиденциальности и контроля над ним. Эти принципы должны включать в себя идентификацию и аутентификацию, авторизацию, аудит, контроль за физическими носителями.

Правила применения методов защиты при передаче классифицированных данных. Эти правила должны быть описаны для всех используемых в компании способов передачи, например, сети передачи данных (локальная, распределенная), электронная почта, факс, телефонные разговоры (включая мобильную связь), бумажные копии, видео конференции, модемная связь, репликации баз данных.

Маркировка и методы хранения классифицированной информации. Правила маркировки должны быть указаны для каждого типа классифицированной информации и для всех используемых в компании способов хранения, включая хранение на серверах, рабочих станциях, ноутбуках, сменных носителях (дискеты, флэш-карты и т.п.).

Порядок уничтожения носителей с классифицированными данными. Должен предусматривать правила уничтожения каждого типа информации на всех типах используемых носителей, включая жесткие диски, сменные носители (дискеты, ленты, флэш-карты и т.д.), электронная почта, бумажные копии.

Правила обращения с классифицированной информацией. Они определяют требования по маркировке, хранению, передаче и уничтожению для каждого типа классифицированных данных.

Фрагменты стандарта классификации данных

Фрагмент правил определения конфиденциальной информации

Гриф «конфиденциальная» должен присваиваться только информации, которая в случае ее разглашения ухудшит конкурентное положение компании, нанесет серьезный финансовый ущерб, приведет к невыполнению нормативных обязательств, понизит общественный престиж или иным способом причинит серьезный вред компании, ее клиентам или партнерам.

Примеры:

- контракты;
- отчеты компании до момента опубликования;
- документы финансового планирования.

Фрагменты стандарта классификации данных, продолжение

Фрагмент требований по идентификации и аутентификации для каждой категории информации

Тип контроля	Типы информации			
	Публичная	Для внутреннего использования	Конфиденциальная	Строго конфиденциальная
Идентификация и аутентификация	■ Не требуется	■ Имя пользователя и пароль	■ Имя пользователя и пароль с контролем качества	■ Двухфакторная аутентификация (смарткарта, токен, сертификат)

Фрагмент предписываемых методов защиты при передаче по компьютерным сетям

Носитель информации	Публичная	Для внутреннего использования	Конфиденциальная	Строго конфиденциальная
Сети передачи данных (локальная, распределенная)	■ Не требуется	■ Управление доступом в сети	■ Шифрование	■ Шифрование

Фрагмент Маркировка для бумажных носителей

Носитель информации	Публичная	Для внутреннего использования	Конфиденциальная	Строго конфиденциальная
Бумажные копии	■ Не требуется	■ На первой странице - гриф «Для внутреннего использования»	■ Все страницы промаркированы грифом «Конфиденциально» ■ Требуется подтверждение доставки ■ Копии хранятся в местах специального хранения	■ Все страницы должны содержать следующую маркировку: «Строго конфиденциально», копия №, страница № ■ Получатель расписывается за получение ■ Запрещается копирование ■ Хранение в сейфах

Фрагменты стандарта классификации данных, продолжение

Фрагмент правил уничтожения носителей с классифицированными данными

Носитель информации	Публичная	Для внутреннего использования	Конфиденциальная	Строго конфиденциальная
Жесткие диски, Сменные носители (дискеты, ленты, флэш-карты и т.д.)	■ Не требуется	■ Удаление файлов	■ Затирание файлов	■ Затирание файлов или физическое уничтожение носителей

Фрагмент правил обращения с конфиденциальной информацией

Категория классификации	Схема обработки информации
Конфиденциальная	**Маркировка**: «Конфиденциально» на всех страницах **Хранение**: в местах специального хранения или в зашифрованном виде **Передача**: двухфакторная аутентификация и шифрование; необходимость отчета о распределении определяется владельцем **Уничтожение**: с помощью шредера, удаление файлов

МЕТОДИКА ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ ИНФОРМАЦИИ

Предлагаемая методика основана на рекомендациях международных стандартов информационной безопасности BS 7799 и ISO 17799.

Процесс разработки корпоративного стандарта классификации информации состоит из следующих основных этапов:

- создание рабочей группы;
- проведение собеседований с подразделениями компании;
- консолидация собранных сведений;
- согласование с подразделениями компании консолидированных сведений и утверждение стандарта.

СОЗДАНИЕ РАБОЧЕЙ ГРУППЫ

От того, насколько правильно сформирована рабочая группа, зависит успех всего мероприятия. В рабочую группу должны входить ответственные

представители подразделений компании и специалисты, обладающие, как минимум, следующими качествами:

- Имеют хорошие знания в отрасли, в которой работает компания, знают структуру компании, особенности данного бизнеса, конкурентов, партнеров по бизнесу.
- Имеют достаточные знания в области информационной безопасности. Хорошим подтверждением наличия необходимых знаний является международный сертификат CISSP.
- Имеют детальное представление об информационных системах компании. Например, пользователи могут хранить важную информацию на диске «P», при этом следует знать, на каком сервере находится этот диск «P» у данного пользователя.
- Имеют отличные навыки проведения собеседований. Это очень важное требование. В отсутствие данных навыков чаще всего случаются упущения в работе, а иногда и отрицательное отношение ко всему проекту со стороны руководства компании и ее сотрудников.
- Обладают навыками делового общения с представителями высшего руководства, которые, как правило, могут выделить лишь малое количество времени для собеседований.
- Пользуются авторитетом и уважением в компании.
- Имеют опыт проведения проектов в области классификации информации. Отсутствие опыта обязательно скажется на качестве результата проекта.

В рабочую группу следует включить представителей всех заинтересованных подразделений, например, подразделения службы безопасности.

ПРОВЕДЕНИЕ СОБЕСЕДОВАНИЙ С ПОДРАЗДЕЛЕНИЯМИ КОМПАНИИ

Как определить, к какой степени конфиденциальности относится тот или иной тип информации? На этот вопрос должен ответить владелец информации. Несмотря на кажущуюся простоту, собрать эти сведения не так просто. Ведь собранные сведения будут ценны только в том случае, если они собраны в достаточном объеме.

Для формирования понимания того, какие виды информации обрабатываются в определенных подразделениях компании, следует провести серию собеседований с ответственными лицами этих подразделений.

До начала собеседований нужно подготовить предварительный список типов данных, свойственный компаниям данной отрасли. Наличие такого списка сократит время, затрачиваемое на проведение собеседований, и поможет избежать упущений.

Все ответственные лица должны быть заранее ознакомлены с принципами классификации информации и предварительным списком типов данных. Для этого нужно провести вводную презентацию для представителей подразделений, в ходе которой разъяснить цели и задачи проекта, рассказать, кто является спонсором (главным заказчиком) проекта, изложить последователь-

ность шагов, объяснить, какое от представителей подразделений требуется участие и каков конечный результат проекта. Презентация также существенно сократит время собеседований, так как сотрудники будут к ним подготовлены.

Обсуждая бизнес-процессы, в которых задействовано подразделение, следует составить список используемых в подразделении типов информации и по каждому из них задать достаточно длинный список вопросов. Вот некоторые из них:

- Какой уровень конфиденциальности, по мнению ответственного лица, может быть присвоен данным, находящимся в его компетенции?
- Где хранятся данные (локальная сеть, почтовый ящик электронной почты, печатная копия и пр.)?
- Как происходит обмен данными внутри компании?
- Какие виды информационного обмена между подразделением и внешними организациями (электронная почта, электронная почта с использованием PGP, печатные копии, факсимильная связь, устное общение) применяет компания?
- Какие методы и средства защиты используются?
- Другие наводящие вопросы.

Часто встречаются ситуации, когда подразделения компании перестраховываются, завышая степень конфиденциальности тех или иных данных. В таком случае следует задать наводящие вопросы, например такой: «Чем выше степень конфиденциальности, тем строже правила работы с ней. Готовы ли вы расписываться в журнале каждый раз при получении данных документов и каждый день сдавать их под роспись?»

Фрагмент списка типов данных компании – оператора связи

- Документы внутреннего регламента компании
- Прайс-листы
- Маркетинговые материалы и прес-релизы (до опубликования)
- Информация об абонентах, клиентах и дилерах
- Счета, выставляемые абонентам, клиентам и дилерам
- Счета, выставляемые поставщикам
- Финансовое планирование и прогнозы
- Информация об инвестициях
- Сведения о зарплате и других вознаграждениях
- Контракты
- Рекрутинг

КОНСОЛИДАЦИЯ СОБРАННЫХ СВЕДЕНИЙ

Проведя собеседования с подразделениями компании, можно переходить к консолидации собранных сведений. Консолидация заключается в присвоении степени конфиденциальности имеющимся типам информации. Мнения

подразделений об этих степенях могут расходиться, в этом случае следует опираться на профессиональное суждение рабочей группы. Иногда требуется провести дополнительные собеседования. В коммерческой компании список конфиденциальной и строго конфиденциальной информации не должен получиться большим. Длинный список свидетельствует об ошибках, допущенных при проведении собеседований.

УТВЕРЖДЕНИЕ СТАНДАРТА

Консолидированный список типов данных и их степени конфиденциальности должен быть согласован с подразделениями компании и утвержден высшим руководством компании в составе документа «Классификация информации по степени конфиденциальности». Наиболее частое препятствие на этом этапе возникает со стороны службы безопасности из-за недоверия с ее стороны к полученным результатам, а также в силу специфики менталитета руководства и специалистов подобных подразделений. Что бы избежать такой ситуации, в процесс проекта и в рабочую группу следует привлекать представителей службы безопасности.

ЧТО ДАЛЬШЕ?

«Классификация информации» задает требования по обращению с данными, но не технические детали, она служит каркасом для документов более «низкого» уровня. Конкретные способы реализации требований по обращению с классифицированной информацией должны определяться в документах более «низкого» уровня в соответствии с требованиями «Классификации», например в инструкциях пользователей и администраторов, стандартов конфигурации рабочих станций и серверов.

О КОМПАНИИ «КЕРБЕРУС»

Наша миссия - защита Ваших информационных активов

«Керберус» - компания, ориентированная исключительно на защиту информационных активов своих клиентов.

Мы предлагаем комплексные решения в области компьютерной безопасности, применительно к индивидуальным потребностям Заказчика. Наша методология, совместно с отлаженными процессами обслуживания клиентов, позволяют нам гарантировать высокое качество оказываемых услуг. Мы стараемся быть лучшими и предоставлять услуги в области компьютерной безопасности только высшего качества.

Наш Опыт

«Керберус» уделяет огромное внимание уровню квалификации сотрудников. Наши специалисты имеют значительный опыт практической работы в банковской отрасли, промышленности, предоставлению профессиональных услуг в области компьютерной безопасности, управлению ИТ инфраструктурой, разработке программного обеспечения. Такой опыт позволяет нам разрабатывать практичные и эффективные решения для защиты Вашего бизнеса.

Менеджеры "Керберус" имеют за плечами успешный опыт развития практики оказания услуг по информационной безопасности в иностранной компании.

Дополнительная информация

Если у Вас возникли вопросы или нужна дополнительная информация, обращайтесь по тел. (095) 792-0358 или по E-mail info@kerberus.ru.