СПИСОК ЛИТЕРАТУРЫ:

1. *Тимонин М. В., Лаврентьев В. С.* Использование теории нечеткой меры для агрегации составляющих риска информационной безопасности (в печати).
2. *Gordon L. A., Loeb M. P.* The Economics of Information Security Investment // ACM Trans. Inf. Syst. Secur., 5(4): 438–457, November 2002.

К. С. Титков

О МЕТОДАХ ОБЕСПЕЧЕНИЯ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ В КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

При построении системы информационной безопасности (ИБ) в организации необходимо предпринять ряд мер по охране конфиденциальности информации (КИ), продиктованных требованиями бизнес-процессов организации и федерального законодательства. В числе прочего эти меры могут включать в себя введение режима коммерческой тайны (КТ), а значит, определение перечня и порядка обращения с информацией, составляющей эту тайну [1]. Однако, в отличие от КТ, порядок защиты профессиональной и других видов тайн не определяется законодательством столь же подробно. Разумным видится применение к прочим видам тайн требований по защите, схожих с требованиями к КТ. Решение данной задачи обеспечивается системой организационных и технических мер, основанной на внутренних нормативных документах организации. Представляется целесообразным дать обзор перечня, взаимосвязи, структуры и состава этих документов.

Для описания системы защиты требуется ввести некоторые уточнения. Во-первых, необходимо определить виды внутренних нормативных документов и упорядочить их по уровню от верхнего к нижнему. Для построения предлагаемой системы внутренних документов зачастую достаточно четырехуровневой модели, состоящей из политик, положений, регламентов и инструкций по защите информации. Во-вторых, введем более общее понятие режима конфиденциальности информации, путем включения в состав конфиденциальной информации не только КТ, но и других видов тайн в соответствии с законодательством [2]. Для целей настоящего исследования будем полагать, что конфиденциальная информация — это информация, в отношении которой организацией установлен режим конфиденциальности. При этом режим конфиденциальности — это режим, позволяющий обладателю конфиденциальной информации при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, а режим КТ — это вид режима конфиденциальности, реализующий определенные законом [1] меры по охране конфиденциальности информации.

Таким образом, далее будет рассматриваться единая система внутренних нормативных документов коммерческой организации, поддерживающая защиту коммерческой тайны и других видов тайн.

Предлагаемые меры по поддержанию режима конфиденциальности должны вписываться в действующую политику ИБ организации, содержащую совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [3]. На основе указанной политики, издаваемой в виде документа верхнего уровня, разрабатывается положение, определяющее режим конфиденциальности в организации.

Данное положение устанавливает общие правила режима конфиденциальности и определяет основные меры по защите информации в целях предотвращения возможного нанесения ущерба организации ее партнерам, клиентам и работникам вследствие несанкционированного использования информации, в отношении которой введен режим конфиденциальности. Положение обычно определяет:

- перечень категорий КИ и описание их состава;
- порядок установления и снятия грифов конфиденциальности, включая порядок нанесения соответствующей маркировки на все виды документов и носителей;
- порядок допуска к конфиденциальной информации, включающий в себя идентификацию, аутентификацию и учет предоставленного доступа к КИ;
- взаимные обязательства организации и работников, связанные с обработкой КИ и закрепляемые в трудовых договорах;
- общий порядок защиты КИ при ее обработке и передаче на бумажных и электронных материальных носителях и по каналам связи, в том числе внешним организациям и государственным органам на основе гражданско-правовых договоров и федеральных законов;
- систему мер по обеспечению контроля сохранности КИ, включая функции ответственных за обеспечение режима конфиденциальности сотрудников и подразделений, порядок проведения расследований и меры ответственности за нарушение требований режима.

В целях уточнения указанного положения могут быть приняты дополнительные регламенты, уточняющие порядок: обработки и защиты отдельных видов КИ, включая персональные данные, взаимодействия внутренних подразделений по вопросам передачи КИ внешним организациям и предоставления КИ государственным органам, предоставления доступа к конфиденциальным информационным ресурсам. Процедуры и действия сотрудников организации подлежат уточнению в тематических инструкциях.

В зависимости от бизнес-процессов организации прикладные инструкции, как документы нижнего уровня, могут подробно описывать конфиденциальный документооборот, правила обращения с электронными материальными носителями и другие процедуры.

В прямой зависимости от положения о режиме конфиденциальности находится документ, определяющий перечень информации, в отношении которой организацией установлен режим конфиденциальности. Выделение этого перечня из положения упрощает внесение в него изменений.

Подводя итог, целесообразно закрепить введение режима конфиденциальности и, при необходимости, коммерческой тайны приказом по организации после принятия мер по защите информации, изложенных в разработанных и утвержденных внутренних документах.

Применение предложенной модели позволяет упорядочить систему нормативной документации, обеспечивающей режим конфиденциальности в организации. Благодаря предложенным обобщениям становится возможным избежать дублирования положений нормативных документов за счет создания единого режима конфиденциальности.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (в ред. от 02 февраля 2006 г. № 19-ФЗ, от 18 декабря 2006 г. № 231-ФЗ, от 24 июля 2007 г. № 214-ФЗ).
2. Указ Президента РФ от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (в ред. от 23 сентября 2005 г.).
3. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.