СЕКЦИЯ 1. ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

ПРОБЛЕМАТИКА ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ В ЮРИСДИКЦИИ РЕСПУБЛИКИ БЕЛАРУСЬ

В.А. Власенко

В ходе анализа проанализированы существующие в мировой практике механизмы закрепления ответственности по обеспечению безопасности и было установлено, что ответственность за обеспечение безопасности с практической точки зрения в Республике Беларусь закрепить крайне сложно. На данный момент существует крайне мало примеров положительной практики по делам связанным с разглашением коммерческой тайны. Основной причиной данного факта является труднодоказуемость факта непосредственного разглашения коммерческой тайны.

Для закрепления ответственности за работником, либо контрагентом рекомендуется использовать несколько документов. В рамках не только трудового, но и гражданского кодекса.

В рамках трудового кодекса в случае нарушений предусматриваются в основном только меры дисциплинарного воздействия, вплоть до увольнения. Возможна компенсация только реального ущерба. Под реальным ущербом понимаются расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение имущества.

В рамках гражданско-правовых отношений можно предусмотреть неустойку, за нарушение правил работы с информационными активами. Одним из примеров таких документов является «Обязательство о неразглашении коммерческой тайны», в рамках которого можно предусмотреть правила работы с документами, определить типы нарушений и установить размер неустойки. Взыскание неустойки осуществляется в судебном порядке, за исключением случаев добровольного перечисления денежных средств на расчетный счет нанимателя. Сумма неустойки может быть уменьшена судом.

Несмотря на возможные способы штрафных мер, наилучшей практикой считается система сокращения премий.

АУДИТ КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

Н.М. Книга, В.П. Ширинский

В настоящее время аудит информационной безопасности (ИБ) представляет собой одно из наиболее актуальных и динамично развивающихся направлений в области безопасности информационных систем (ИС).

Его основная задача — оценить текущее состояние ИБ компании, ее адекватность поставленным целям и задачам бизнеса. Поэтому под аудитом ИБ корпоративной системы обычно понимается системный процесс получения качественных и количественный оценок о текущем состоянии ИБ компании в соответствии с определенными критериями и показателями безопасности.

Этот системный процесс включает в себя следующие шаги:

– описание и оценку текущего уровня защищенности ИС;

– анализ рисков, связанных с возможностью осуществления внутренних и внешних угроз в отношении ресурсов ИС;

– рекомендации по повышению уровня безопасности системы (устранение уязвимостей, разработка политики информационной безопасности).