ОБОСНОВАНИЕ НОВЫХ ПРИНЦИПОВ ПРОВЕДЕНИЯ АУДИТА СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

В.А. Бойправ, Л.Л. Утин

Установлено, что основными недостатками при проведении аудита систем менеджмента информационной безопасности (СМИБ) организаций являются следующие:

- необходимость выполнения интеграции принятых на территории Республики Беларусь международных стандартов, регламентирующих аудит СМИБ, и национальных технических, нормативных и правовых актов (ТПНА) в сфере защиты информации;
- противоречивость требований принятых на территории Республики Беларусь международных стандартов, регламентирующих аудит СМИБ, и требований национальных ТНПА в сфере защиты информации, что затрудняет как процесс интеграции документов указанных видов, так и процесс их одновременного использования в ходе проведения аудита СМИБ;
- исключение из процесса аудита СМИБ сотрудников и персонала, участвующих в создании информационной инфраструктуры организации;
- низкая заинтересованность руководителей организации в проведении аудита СМИБ и слабая их вовлеченность в этот процесс, вследствие чего руководители, как

правило, ориентированы на снижение затрат как на регулярное проведение аудита СМИБ, так и на устранение обнаруженных в ходе аудита недостатков этой системы;

- высокий уровень затрат временных и человеческих ресурсов на проведение аудита СМИБ (как внутреннего, так и внешнего), что обусловлено как вышеперечисленными недостатками, так и отсутствием средств для автоматизации этого процесса.

Для нивелирования указанных недостатков авторами предложено дополнить существующие принципы проведения аудита СМИБ, представленные в ISO/IEC 27007:2020 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие положения по проведению аудита систем менеджмента информационной безопасности», принципами, обоснованными в работе [1], а также нижеследующими принципами.

1. Принцип всеохватываемости. В соответствии с этим принципом в процессе аудита должны быть задействованы не только работники аудируемой организации, которые в рамках выполнения своих должностных обязанностей используют информационную систему, но и работники, которые обеспечивают создание и эксплуатацию инфраструктуры для этой системы.

2. Принцип оптимизации. В соответствии с этим принципом необходимо принимать все возможные меры для сокращения временных и человеческих ресурсов на проведение аудита путем. Для этого необходимо использовать специальные программные средства для проведения аудита и опросные листы для сотрудников аудируемой организации, составленные на основе принципа разумной достаточности.

3. Принцип своевременности. В соответствии с этим принципом проведение аудита должно проводить как на регулярной, так и на внеплановой основе. Внеплановое проведение аудита СМИБ целесообразно реализовывать после издания новых нормативных документов в сфере защиты информации или внесения изменений и дополнений в такие документы.

Литература

1. Бойправ В.А., Утин Л.Л. Принципы реализации методики аудита системы менеджмента защиты информации в организациях электросвязи // Доклады БГУИР. 2016. № 6 (100). С. 94–99.