(организации категории 1), предоставление услуг электросвязи (организации категории 2), проектирование сетей электросвязи (организации категории 3), управление и регулирование деятельности организаций электросвязи (организации категории 4). Вопросы составлены с учетом требований к системе защиты информации, изложенных в Приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62, а также положений СТБ ISO/IEC 27001-2016.

Сотрудники, которых следует отнести к кругу лиц, подлежащих опросу в ходе аудита системы менеджмента защиты информации организаций электросвязи: руководитель и/или главный инженер; начальник службы безопасности; старшие производители работ или начальники строительных участков (в случае, если аудируемая организация относится к категории 1); начальники отделов, сотрудники которых работают с электронными документами и базами данных, в которых содержится информация ограниченного распространения (в случае, если аудируемая организация относится к категории 2, 3 или 4).

Из составленных авторами статьи анкетных вопросов для руководителей и/или главных инженеров организаций электросвязи категорий 1–4 можно выделить следующие основные:

1. Выполнена ли классификация КВОИ, доступ к которым имеют сотрудники Вашей организации? 2. Выполняется ли в Вашей организации классификация активов КВОИ, доступ к которым имеют сотрудники? 3. Внедрена и используется ли в Вашей организации политика информационной безопасности? 4. Назначено ли в Вашей организации лицо, на которое возложены обязанности по контролю за соблюдением положений политики информационной безопасности? 5. Осведомляются ли увольняемые сотрудники Вашей организации, которые имели доступ к информации ограниченного распространения, об ответственности, к которой они могут быть привлечены вследствие разглашения этой информации третьим лицам?

СИСТЕМА МОНИТОРИНГА И КОРРЕЛЯЦИЙ СОБЫТИЙ

Ю.О. Быханьков

Для построения эффективной системы защиты информации не только следует разобраться в требованиях законодательства, но и соизмерить их с финансовыми возможностями организации, а также определить механизм мониторинга и аудита информационной безопасности. На текущий момент в Республике Беларусь необходимость в системе мониторинга и корреляций событий следует из регулирующих приказов Оперативно-аналитического центра при Президенте Республики Беларусь и действующих, но местами неработающих и даже противоречащих законодательству стандартов серии 34.101. В виду того что требования к системе защиты информации закреплены, иногда возможно изменить класс объекта информатизации (информационной системы), чтобы уменьшить затраты на построение системы защиты информации, например сокращением средств на реализацию требований пп. 39, 40, 46 приказа № 62 ОАЦ, а в некоторых случаях на разработку и оценку задания по безопасности. Требования по сбору, просмотру и анализу событий безопасности являются обязательными в Республике Беларусь для систем защиты информации независимо от формы собственности. Уменьшение средств защиты может не только навредить безопасности, но и помочь, сфокусировав внимание специалиста. В списке сертифицированных средств уже существуют продукты для адекватного исполнения требований по анализу событий, в то же время существуют варианты формального выполнения пунктов требований регулятора, которые не могут сравниться с системами корреляций событий. В том же приказе прописывается анализ событий уполномоченными субъектами, однако как показывают исследования, квалифицированные субъекты без специальных средств не могут выполнять анализ на должном уровне в режиме реального времени, особенно анализ логов с различных элементов инфраструктуры, что является критически важным для обеспечения защиты информации.

Литература

1. Закон Республики Беларусь Об информации, информатизации и защите информации от 10 ноября 2008 г. № 455-З.

2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62.