УДК 621.9

РАЗРАБОТКА ИНСТРУКЦИЙ ПО СОЗДАНИЮ ПРОЦЕССА АНАЛИЗА УРОВНЯ ЗАЩИТЫ НА ОСНОВЕ ОТКРЫТЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ ДЛЯ ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ

А. А. ВИТЕЛЮЕВА
Научный руководитель А. А. ТЮТЮННИК, канд. экон. наук, доц.
Филиал «Национальный исследовательский университет «МЭИ»
в г. Смоленске
Смоленск, Россия

Получение информации всегда было связано с деятельностью людей и является наиглавнейшим ресурсом технического, а также научного мирового сообщества. Предпринимательская или государственная деятельность предполагает различное использование информационных потоков.

Действенный метод по защите информационной безопасности (ИБ) нужно начинать с применения информационных отношений субъектами, причем для каждого субъекта индивидуальный, но объективно связанный с использованием информационных систем (ИС). Из этого следует, что контроль исследования ИБ организаций, созданных на основе открытых источников, крайне необходим. Если учесть особенности различных сфер деятельности и процесса производства, то процесс АЗООИ должен пройти в соответствии с требованиями отраслей.

Опираясь на данные Positive Technologies, под угрозой, как правило, чаще всего находятся государственные учреждения, а более частые атаки производятся на инфраструктуру, веб-ресурсы, а также на отдельных пользователей. Аналитический отчет экспертного центра безопасности выявил, что наибольшие атаки были направлены на конфиденциальную информацию. Правительственные сайты часто атакуют так называемые хактивисты и это также ощутимо в общих исследованиях.

ИС, которые относятся к государственным информационным системам (ГИС), применяется приказ ФСТЭК 17, в котором содержатся ряд требований по оценке защиты ГИС всех классов и следующие меры.

1. Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей.
2. Контроль установки обновлений ПО.
3. Контроль работоспособности, параметров настройки и правильности функционирования ПО и средств защиты информации.
4. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС.

Подводя итог вышесказанному, предложенные методы можно использовать формально к требованиям регулятора, но в связи с тем, что многое совершенствуется, а сбор информации ограничен, рекомендовано не полагаться на методы АЗООИ как единственно верные.