Тема

Анализ политики информационной безопасности

Автор

Мазяр Алексей Николаевич, 21213

Введение

Ознакомившись с политикой информационной безопасности, прикреплённой к заданию, мне удалось выделить несколько достоинств и недостатков этого документа. Стоит отметить, что документ показался мне сложным для чтения и полным абстрактных терминов и рекомендаций, что я не посчитал недочётом. Видимо такое наполнение продиктовано целью документа, которая, к сожалению, в нём не указана.

Плюсы

Главный плюс документа - то, что он затрагивает практически все пункты начального планирования защиты информации. Например, уделяется внимание лицам ответственным за организацию защиты информации - СИБ. Также определяются возможные угрозы - есть даже перечень внешних и внутренних угроз. Помимо этого в документа перечилсены необходимые защитные меры для противодействия им - этому посвящены все пункты 4.2.3.*. Конечно, не всё расписано в подробностях, зато предоставлены документация и инструкции, связанные с организацией и эксплуатацией средств ИБ - пункт 4.2.1. Более того, в подробности описываются действия по мониторингу информационной безопасности - например пункт 4.2.3.9 содержит ряд подпунктов(например “в.)”), дающих список требований к поддержанию работы инфраструктуры.

Минусы

Одним из сомнительных решений в документе я считаю предложение: “За сохранность рассматриваемых ресурсов отвечают их владельцы”. Возможно я неправильно понимаю понятие “владельцев”, но и их определения не было указано в документе. Проблема этого решения в том, что пользователи, очевидно являясь владельцами своих персональных данных, становятся ответственными за их сохранность. Скорее всего пользователи не хотят быть ответственными за утечку своих персональных данных в случае, например, саботажа внутри организации. Предлагается изменить или разъяснить такое решение, чтобы было ясно, кого в организации считать ответственным за ресурсы, в частности ПДн.

Также в документе ничего не сказано про выбор, приобретение, внедрение и эксплуатацию защитных средств. Нигде не прописывается план действий по

проектированию архитектуры ИБ, то есть в данной ПИБ не уточняется стоит ли рассматривать только сертифицированные решения и можно ли разрабатывать собственные решения. Из всего документа только пункт 4.2.3.4 говорит про услуги третьих лиц, но только с точки зрения эксплуатации. Рекомендуется добавить инструкцию по планированию разработки или приобритению защитных средств.

Более того, не указана система оценки актуальности угроз и ценности ресурсов. Эти параметры необходимы, чтобы определить требования по защите. Кажется, что какая-то система классификации ресурсов и рисков есть, так как употребляются такие выражения, как “Требуемый уровень информационной безопасности” и “... уменьшения рисков до приемлемого уровня”. Для того, чтобы внести ясность в этот шаг планирования ИБ, нужно указать, определять необходимые для реализации требования. Например, можно явно сослаться на упомянутое в 4.2.1 Постановление Правительства РФ от 01.11.2012 № 1119, которое описывает классах защищенности систем .