АЛЬТЕРНАТИВНЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ В МАСШТАБАХ ОДНОГО ВЕДОМСТВА

ЛЕВЧУК ИВАН ЕВГЕНЬЕВИЧ

СОТРУДНИК УПРАВЛЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОСУДАРСТВЕННОГО ПОГРАНИЧНОГО КОМИТЕТА РЕСПУБЛИКИ БЕЛАРУСЬ

Основные НПА по ТЗИ

- Закон Республики Беларусь от 10 ноября 2008 г. № 455-З "Об информации, информатизации и защите информации"
- Закон Республики Беларусь от 28 декабря 2009 г. № 113-З "Об электронном документе и электронной цифровой подписи"
- Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 "О некоторых мерах по совершенствованию защиты информации"
- Указ Президента Республики Беларусь от 9 декабря 2019 №449 "О совершенствовании регулирования в области защиты информации"
- Постановление Совета Министров Республики Беларусь от 12 августа 2014 г. № 783 "О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну"
- Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 16 ноября 2010 г. № 82 "Об утверждении Инструкции о порядке согласования выполнения работ и (или) оказания услуг, составляющих деятельность по технической и (или) криптографической защите информации, в государственных органах и государственных организациях"
- Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 "О некоторых вопросах технической и криптографической защиты информации"
- Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12 марта 2020 г. № 77 "О подтверждении соответствия средств защиты информации"

Необходимо реализовать

- Должно быть создано подразделение технической защиты информации, либо назначено должностное лицо, которое будет ответственными за техническую защиту информации
- Должны быть определены информационные системы, для которых необходимо выполнить мероприятий по обеспечению их информационной безопасности
- Для данных систем или их совокупности необходимо создать, аттестовать и в дальнейшем применять систему(ы) защиты информации

Система защиты и информации

- наличие и выполнение регламентов и инструкций по ИБ для пользователей, технического персонала и специалистов ИБ
- наличие и применение определенного набора средств защиты информации
- соблюдение требований по настройке сетевого, серверного оборудования, системного и специального программного обеспечения, баз данных и других средств обработки информации

Средства защиты информации

- обязательно - антивирусное программное обеспечение
- обязательно - средства предоставления сетевых сервисов (NFW, IPS/IDS, WAF, Sandbox и т.п.)
- обязательно - средства криптографической защиты информации (ЭЦП, IPsec, TLS и т.п.)
- при использовании определенных технологий - средства виртуализации и системы управления сайтами
- а еще желательно - DLP, SIEM, IRP, IDM, PAM и т.п.

Проблемные вопросы

- **Штатные должностные лица, ответственные за техническую защиту информации**
- **Внедрение и эксплуатация средств защиты информации**

Центр технической защиты информации

- Формирование набора средств защиты информации, в т.ч. с включением в него решений Open Source, достаточного для решения задач по обеспечению кибербезопасности для информационных систем, владельцами которых являются госорганы и госпредприятия
- Проведение обследования информационно-коммуникационной инфраструктуры госорганов и госпредприятий, на предмет согласованного с ними внедрения и в дальнейшем обеспечения функционирования средств защиты информации
- Оказание услуг по внедрению и эксплуатации средств защиты информации

СПАСИБО ЗА ВНИМАНИЕ

Левчук Иван Евгеньевич

levchuk_ie@ops.gov.by