Тема 13

Комплексный подход при организации защиты информации

Содержание темы

- Методы оценки эффективности средств обеспечения информационной безопасности.
- Комплексный подход при обеспечении защиты информации.
- Политика безопасности информационных систем.
- Концепция национальной безопасности Республики Беларусь.
- Концепция информационной безопасности Республики Беларусь.

Комплексная ЗИ

Комплексная система защиты информации создается для защиты от наиболее вероятных угроз и охватывает следующие вопросы:

- разработка правового обеспечения ЗИ;
- определение потенциальных угроз безопасности информации;
- составление перечня данных, подлежащих защите;
- создание подразделения, ответственного за вопросы ЗИ;
- определение основных направлений обеспечения информационной безопасности.

Комплексная ЗИ

Все методы защиты информации по характеру проводимых действий можно разделить:

- на законодательные (правовые);
- организационные;
- технические;
- комплексные, включающие элементы всех предыдущих.

Комплексная ЗИ

В Республики Беларусь была выделена особая категория информационных систем – **критически важные объекты информатизации** (**КВОИ**).

Комплексная ЗИ

В соответствии с Указом Президента Республики от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации» **КВОИ** – объект информатизации, который на основании критериев отнесения объектов информатизации к критически важным объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр критически важных объектов информатизации.

Методы оценки эффективности

Оценка эффективности функционирования комплексной системы защиты информации представляет собой сложную задачу. В процессе разработки такой системы используется метод синтеза путем согласованного объединения блоков, устройств, подсистем с последующим анализом эффективности полученного решения. Анализ осуществляется с помощью моделирования, по результатам которого из множества синтезированных систем выбирается лучшая. Реализация модели позволяет получать и исследовать характеристики реальной системы.

Методы оценки эффективности

Эффективность систем оценивается с помощью показателей эффективности, которые характеризует степень соответствия оцениваемой системы своему назначению. В оценке эффективности комплексной системы защиты информации, в зависимости от используемых показателей эффективности и способов их получения, выделяют:

классический,

официальный и

экспериментальный подходы.

Методы оценки эффективности

Под **классическим подходом** к оценке эффективности понимается использование критериев эффективности, полученных с помощью показателей эффективности. Значения показателей эффективности получаются путем моделирования или вычисляются по характеристикам реальной системы.

Методы оценки эффективности

Официальный подход к определению эффективности комплексных систем защиты информации опирается на нормативные акты, в которых определены требования по защите информации.

Требования могут задаваться перечнем механизмов защиты информации, которые необходимо иметь или реализовать в компьютерной системе, чтобы она соответствовала определенному классу защиты.

Методы оценки эффективности

В настоящее время в Республике Беларусь официальный подход к оценке эффективности системы защиты информации регламентируется приказом Оперативно-аналитического центра при Президенте Республики Беларусь № 66 от 20 февраля 2020 года «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449», в котором описаны классы типовых информационных систем, приведен перечень требований к системе защиты информации, подлежащих включению в техническое задание, а также представлены требования к организации взаимодействия информационных систем.

Методы оценки эффективности

Под **экспериментальным подходом** понимается организация процесса определения эффективности существующих комплексных систем защиты информации путем попыток преодоления защитных механизмов системы специалистами, выступающими в роли злоумышленников.

Такой подход к оценке эффективности позволяет получать объективные данные о возможностях существующих систем защиты, но требует высокой квалификации исполнителей и больших материальных и временных затрат.

Политика безопасности

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которым руководствуется организация в своей деятельности.

Политика безопасности

Согласно СТБ ISO/IEC 27001-2016 высшее руководство должно установить политику информационной безопасности, которая:

- соответствует назначению организации;
- включает цели (задачи) в области информационной безопасности, или служит основой для задания таких целей (задач);
- включает обязательство соответствовать действующим требованиям, связанным с информационной безопасностью;
- включает обязательство непрерывного улучшения системы менеджмента информационной безопасности.

Политика безопасности

Политика безопасности устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Она должна:

- быть оформлена как документированная информация;
- быть доведена до сведения сотрудников в организации;
- быть доступной в установленном порядке для заинтересованных сторон.

Политика безопасности

Фундаментом для создания системы защиты информации является документ, в котором формулируются принципы и основные положения политики предприятия в области информационной безопасности.

Документацию политики безопасности разделяют на документацию:

верхнего,

среднего и

нижнего уровней.

Политика безопасности

Документы верхнего уровня политики информационной безопасности отражают позицию организации к деятельности в области защиты информации, её стремление соответствовать государственным, международным требованиям и стандартам в этой области.

Политика безопасности

К среднему уровню относят документы, касающиеся отдельных аспектов информационной безопасности. Это требования на создание и эксплуатацию средств защиты информации, организацию информационных и бизнес-процессов организации по конкретному направлению защиты информации.

Политика безопасности

В политику информационной безопасности нижнего уровня входят регламенты работ, руководства по администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности.

Концепция национальной безопасности

Действующая в настоящее время Концепция национальной безопасности Республики Беларусь утверждена Указом Президента Республики от 09.11.2010 № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» и дополнена Указами Президента Республики от 30.12.2011 № 621 и от 24.01.2014 № 49.

Концепция национальной безопасности

Концепция национальной безопасности Республики Беларусь закрепляет совокупность официальных взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз.

Концепция национальной безопасности

Данная концепция охватывают:

политическую,

экономическую,

научно-техническую,

социальную,

демографическую,

информационную,

военную и

экологическую сферы жизнедеятельности личности, общества и государства.

Концепция национальной безопасности

В концепции указано, что информационная сфера превращается в системообразующий фактор жизни людей, обществ и государств.
Информационные технологии нашли широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями.

Концепция национальной безопасности

Основными национальными интересами в информационной сфере, которые касаются вопросов информационной безопасности, являются:

- преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
- обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

Концепция национальной безопасности

Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.

Концепция инфор-ой безопасности

Концепция информационной безопасности Республики Беларусь утверждена Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь».

Концепция инфор-ой безопасности

Концепция представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности.

Концепция инфор-ой безопасности

В данной концепции отмечено, что на нынешнем этапе мирового развития информационная сфера приобретает ключевое значение для современного человека, общества, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах.

Концепция инфор-ой безопасности

Повсеместное функционирование объектов промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности. Кибератаки на информационную инфраструктуру рассматриваются в мире как одна из наиболее значимых угроз безопасности.