ОБЗОР ЗАКОНОДАТЕЛЬСТВА И НОРМАТИВНЫХ ТРЕБОВАНИЙ В ОБЛАСТИ АТТЕСТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ

Е.В. Колосовский, А.Н. Марков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В наше время особое значение имеет организация безопасности информационных систем, особенно в государственных системах и системах, обрабатывающих конфиденциальную информацию. Аттестация этих систем проводится Оперативно-аналитическим центром при Президенте Республики Беларусь согласно приказам [1]. В приказах регламентируется законодательные нормы и требования к безопасности систем.

Законодательные и нормативные требования в области аттестации информационных систем отличаются в зависимости от класса информационной

системы. Так информационные системы выделяют в зависимости от типа обрабатываемой информации, того, является ли система государственной, имеет ли доступ к открытым каналам данных.

Общий перечень требований включает в себя аудит безопасности, требования по обеспечению защиты данных, требования по обеспечению идентификации и аутентификации, требования по защите системы защиты информации информационной системы, обеспечение криптографической защиты информации, дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре и иные требования.

Требования отличаются в зависимости от типов систем. Так, для некоторых типов систем «обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года» входит в список обязательных требований, а для классов 4-ин, 4-спец, 4-юл, 4-дсп и 3-юл является рекомендуемой частью аудита безопасности.

В ходе аудита составляется акт, в котором каждому вопросу выставляется отметка о выполнении, номер, дата, наименование документа в котором реализованы требования. Обязательным для всех классов систем является этап с составлением требований по обеспечению защиты данных, в рамках которых проводится регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием, и обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности [2].

Список литературы

1. Приказы оперативно-аналитического центра при Президенте Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/law/orders-of-the-oac. – Дата доступа: 07.05.2024.

2. Приказы оперативно-аналитического центра при Президенте Республики Беларусь о технической и криптографической защите персональных данных [Электронный ресурс]. – Режим доступа: https://www.oac.gov.by/public/content/files/files/law/prikaz-oac/2021-195.pdf. – Дата доступа: 07.05.2024.