ВЗАИМОСВЯЗЬ ТИПОВОГО КЛАССА ИНФОРМАЦИОННОЙ СИСТЕМЫ И ДАЛЬНЕЙШИХ ЭТАПОВ ЕЕ АТТЕСТАЦИИ

Сергеенко М.С., Дворникова Т.Н.

Белорусский Государственный университет информатики и радиоэлектроники г. Минска Республики Беларусь, 2022 год.
Минск, Республика Беларусь, 2022 г.

В данной работе представлены результаты исследования взаимосвязи выбора типового класса информационной системы на предоставляемые требования к системе защиты информации, а также методике и плану ее аттестации.

This paper presents the results of a study of the relationship between the choice of a typical class of an information system and the provided requirements for an information security system, as well as the methodology and plan for its certification.

ВВЕДЕНИЕ

В соответствии с требованиями [1] информация, обрабатываемая в государственных информационных системах (далее – ИС) обязана иметь аттестованную систему защиты информации (далее – СЗИ)., в порядке, установленном Советом Министров Республики Беларусь.

Аттестация систем защиты информации ИС – необходимое условие функционирования систем должным образом. Системы, подвергающиеся данному процессу, предназначены как для обработки, хранения и предоставления информации ограниченного распространения, так и для общедоступной информации.

Процесс аттестации проводиться в следующих случаях: создание СЗИ, продление аттестата соответствия, изменение технологии обработки защищаемой информации.

Аттестация – трудоемкий процесс, в основе которого лежит комплекс организационно-технических мероприятий с документальным подтверждением соответствия системы требованиям законодательства. Аттестация состоит из множества пунктов, которые приведены в [3], каждый из которых имеет свое документированное заключение. Стоит отметить, что до процесса аттестации необходимо вначале создание СЗИ, которое является основополагающим в данной цепочке.

Классификация информационных систем. Требования к СЗИ напрямую зависят непосредственно от характеристик и предназначения самой ИС. Для возможности выделения каких-то общих требований к ИС, а следовательно проведения их аттестации, необходимо каким-то образом ИС сгруппировать по схожим критериям. Классификация информационных систем, учитывающая их предназначения, циркулирующую информацию и взаимодействия приведена в [2]. Однако, в данном стандарте Беларуси представлена она не в полном объеме. В Положении о порядке технической и криптографической защиты информации и информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра (далее – ОАЦ) при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 (в редакции приказа от 12.11.2021 №195) классификация типовых информационных систем представлена в полном объеме.

Первым пунктом в создании СЗИ является анализ циркулирующей информации в ИС, далее же создается акт отнесения ИС к типовому классу, что является ключевым моментом, как в создании системы защиты информации, так и аттестации той же системы, так как первоочередной задачей процесса аттестации является проверка отнесения ИС к типовому классу. Почему это так важно и почему данному моменту уделяется так много внимания? На практике встречаются ситуации, когда не совсем понятно к какому типовому классу отнести рассматриваемую ИС, что заставляет задуматься о направлении политики безопасности организации, особенностей ее деятельности и к чему она хочет прийти в области информационной безопасности, ведь именно от выбранного класса ИС будут зависеть следующие шаги.

Требования к ИС. После определения типового класса ИС необходимо составить Задание по безопасности на СЗИ (далее – ЗБ), либо же Техническое задание на нее. Что именно большой роли не играет, так как суть остается одинаковой. Данный документ является основополагающим для процесса аттестации ИС, так как именно он содержит требования к рассматриваемой информационной системе. Но откуда данные требования возникают? Необходимо опять вернуться к типовым классам ИС. В [3] для каждого класса подробно расписаны требования как к самим ИС, так и к их взаимодействию с другими системами. Именно данная структура является основой для создания ЗБ, естественно помимо данных требований необходимо обращать внимание на специфику ИС, работы организации и прочие вещи, однако данные критерии являются основополагающими, от которых отталкиваемся.

Методика аттестации. Первым пунктом в аттестации информационных систем является создание программы аттестации. Программа аттестации ИС – документ, определяющий последовательность действий в данном масштабном процессе. К нему стоит подходить обдуманно и внимательно, максимально учитывать особенности, рассматриваемой ИС, обращая внимание на возможные угрозы СЗИ системы или же модель нарушителя, если она представлена в виде отдельного документа на СЗИ или же в ЗБ. Программа аттестации содержит в себе последовательность действий с их характеристикой и сроками, помогая осознать объем работ и структурировать действия.

Следующим пунктом идет Методика испытаний системы защиты информации на соответствие требованиям безопасности в реальных условиях эксплуатации. Данный документ является ядром аттестации и включает в себя все предыдущие. Он включает в себя краткое описание ИС, требования, отраженные в ЗБ, так и, соответственно, типовой класс системы. На основании Программы аттестации ИС, учитывая ранее перечисленное, необходимо продумать испытания ключевых моментов СЗИ, проверить выполнения всех условий сохранения информационной безопасности ИС, выполнения соответствия ИС законодательству, включая во внимания помимо технических аспектов, также организационные.

ЗАКЛЮЧЕНИЕ

Таким образом, в данном тезисе отражена взаимосвязь между этапами как создания СЗИ, так и самого процесса аттестации системы.

Аттестация помимо технических аспектов реализации системы защиты информации в целях обеспечения информационной безопасности как непосредственно ИС, так и организации в целом, проверяет и организационные аспекты, что в конечном счете дает понять общую картину и политику информационной безопасности, которой придерживается организация. Таким образом, аттестат соответствия СЗИ ИС отображает кредит доверия к организации, так как до того, как его получить СЗИ проходит множественные проверки, отображенные в методике аттестации, на соответствия требованиям, которые выдвигаются в соответствии с типовым классом рассматриваемой ИС.

Список использованных источников: [1] Закон Республики Беларусь от 10 ноября 2008 г. 455-З «Об информации, информатизации и защите информации»;

[2] СТБ 34. 101. 30-2017 Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация;

[3] Положение о порядке технической и криптографической защиты информации и информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 (в редакции приказа от 12.11.2021 №195).