УДК 621.3.049.77-048.24:537.2

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ. О РЕАЛИЗАЦИИ УКАЗА ПРЕЗИДЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ №40

Волкова А.А., Завтур А.А.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Калита О.В. – магистр, ст. преподаватель, ученый секретарь кафедры ПИКС

Аннотация. Проектирование системы защиты информации в соответствии с приказом №66 ОАЦ при Президенте Республики Беларусь. Интеграция с приказом Президента Республики Беларусь №40. Создание центров оперативного реагирования для критически важных объектов информатизации.

Ключевые слова: система защиты информации, критически важный объект информатизации, центры кибербезопасности.

Введение. Комплекс мероприятий по обеспечению защиты информации и кибербезопасности строго регулируется государством. Нормативная база в данной сфере обновляется достаточно часто, так как сфера новая и не полноценно изученная. Для критически важных объектов информатизации (далее - КВОИ) применяются особые требования.

В данной статье рассмотрен новый приказ главы государства об обеспечении кибербезопасности для КВОИ.

Основная часть. Согласно приказу Оперативно-аналитического центра, при президенте Республики Беларусь 20.02.2020 №66 [1]:

Комплекс мероприятий по технической и криптографической защите информации, подлежащей обработке (сбору, накоплению, вводу, выводу, приему, передаче, записи, хранению, регистрации, уничтожению, преобразованию, отображению) в информационной системе, включает:

– проектирование системы защиты информации;

– создание системы защиты информации;

– аттестацию системы защиты информации в соответствии с Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденным приказом, утверждающим настоящее Положение;

– обеспечение функционирования системы защиты информации в процессе эксплуатации информационной системы;

– обеспечение защиты информации в случае прекращения эксплуатации информационной системы.

На этапе проектирования системы защиты информации осуществляются:

– анализ структуры информационной системы и информационных потоков (внутренних и внешних) в целях определения состава (количества) и мест размещения элементов информационной системы (аппаратных и программных), ее физических и логических границ;

– издание политики информационной безопасности. При этом физическое лицо, являющееся собственником (владельцем) информационной системы, в которой обрабатываются персональные данные, за исключением индивидуального предпринимателя, вправе не издавать политику информационной безопасности;

– определение требований к системе защиты информации в техническом задании на создание системы защиты информации (далее – техническое задание);

– выбор средств технической и криптографической защиты информации; разработка (корректировка) общей схемы системы защиты информации.

Однако, в соответствии с указом Президента Республики Беларусь 14.02.2023 №40 [2], для КВОИ необходимо создать центры обеспечения кибербезопасности и реагирования на киберинциденты.

Перечень владельцев КВОИ приведен в приложении 1 к Указу Президента Республики Беларусь 14.02.2023 №40 [2]. Указом Президента Республики Беларусь 16.04.2013 №196 [3] утверждено положение о порядке отнесения объектов информатизации к критически важным объектам информатизации.

Согласно Указу Президента Республики Беларусь 14.02.2023 №40 [2]:

3.5. владельцы критически важных объектов информатизации, указанные в приложении 1, а также уполномоченные поставщики интернет-услуг, оказывающие услуги хостинга официальных интернет-сайтов и электронной почты, обеспечивают создание центров кибербезопасности в срок не позднее одного года со дня вступления в силу настоящего пункта;

3.7. до начала функционирования центры кибербезопасности подлежат аттестации, проводимой ОАЦ. В последующем аттестация проводится с периодичностью не реже одного раза в три года. Порядок проведения аттестации определяется ОАЦ;

3.8. центры кибербезопасности:

– осуществляют автоматизированные сбор, обработку, накопление, систематизацию и хранение данных о кибербезопасности объектов информационной инфраструктуры, направленные на обнаружение, предотвращение и минимизацию последствий кибератак, а также мероприятия по выявлению, предупреждению и исследованию кибератак и вызванных ими киберинцидентов на указанных объектах, реагированию на такие киберинциденты;

– проводят оценку степени защищенности объектов информационной инфраструктуры, мероприятия по установлению причин киберинцидентов, вызванных кибератаками на объекты информационной инфраструктуры;

– осуществляют сбор, обработку, анализ и обобщение информации о состоянии кибербезопасности на объектах информационной инфраструктуры;

– информируют Национальный центр кибербезопасности о выявленных киберинцидентах не позднее одного часа с момента их выявления, а также представляют в указанный центр иные сведения, в том числе о результатах реагирования и ликвидации последствий киберинцидента в порядке, объеме и сроки, определяемые ОАЦ;

– обеспечивают функционирование в своем составе команд реагирования на киберинциденты;

3.9. центры кибербезопасности организуют не реже одного раза в три года в республиканском унитарном предприятии «Национальный центр обмена трафиком» обучение своих работников, в обязанности которых входит обеспечение кибербезопасности, по образовательной программе повышения квалификации руководящих работников и специалистов по вопросам кибербезопасности.

Согласно Указу Президента Республики Беларусь 14.02.2023 №40 [2] в стране должны быть создана национальная система обеспечения кибербезопасности, элементами которой являются:

Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ);

Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты (далее – Национальный центр кибербезопасности);

– центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности);

– оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций (далее – авторизованный оператор электросвязи);

– объекты информационной инфраструктуры государственных органов и иных организаций (далее – объекты информационной инфраструктуры);

– сети передачи данных, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности, указанных в абзацах втором–пятом настоящего пункта.

Задачами национальной системы обеспечения кибербезопасности являются:

– достижение максимальной скоординированности действий государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры;

– постоянный поиск потенциальных уязвимостей национального сегмента глобальной компьютерной сети Интернет;

– проведение анализа информации о кибератаках и вызванных ими киберинцидентах, установление причин киберинцидентов;

– оценка эффективности защищенности объектов информационной инфраструктуры от кибератак;

– прогнозирование ситуации в области обеспечения кибербезопасности.

Заключение. Рассмотрено требование к обеспечению информационной безопасности для КВОИ. Можно сделать вывод, что создание центров оперативного регулирования в данный момент является насущной проблемой, так как до сегодняшнего дня не вышли пояснения, какие именно функции должны выполняться данными центрами.

Список литературы

1. Приказ Оперативно-аналитического при Президенте Республики Беларусь 20 февраля 2020 г. №66 «О мерах реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. №449». – Минск, 2020 г. – 54 с.

2.Указ Президента Республики Беларусь от 14 февраля 2023 г. №40 «О кибербезопасности». – Минск, 2023 г. – 11 с.

3.Указ Президента Республики Беларусь от 16 апреля 2013 г. №196 «О некоторых мерах по совершенствованию защиты информации». – Минск, 2013 г. – 15 с.

UDC 621.3.049.77–048.24:537.2

DESIGN OF INFORMATION PROTECTION SYSTEMS ON CRITICALLY IMPORTANT INFORMATION OBJECTS. ON THE IMPLEMENTATION OF THE DECREE OF THE PRESIDENT OF THE REPUBLIC OF BELARUS No. 40

Volkova A.A., Zavtur A.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Kalita O.V. – master, senior lecturer, scientific secretary of the Department of ICSD

Annotation. Designing an information security system in accordance with order No. 66 of the OAC under the President of the Republic of Belarus. Integration with the order of the President of the Republic of Belarus No. 40. Creation of rapid response centers for critical informatization objects.

Keywords: information security system, critically important object of informatization, cybersecurity centers.