Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. Том 2 (68). 2016 г. № 2. С. 15–19.

УДК 004.056.5

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Бойченко О. В., Аношкина А. А.

Крымский федеральный университет имени В. И. Вернадского, Симферополь, Российская Федерация
E-mail: bolek61@mail.ru

В статье исследованы характеризующиеся интенсивно возрастающей ролью информационной сферы проблемы по предупреждению и ликвидации угроз информационной безопасности Российской Федерации. Изучены основные источники угроз информационной безопасности, определены способы и методы обеспечения безопасности критически важных объектов. Предложен ряд правовых и организационных мер, направленных на обеспечение безопасности инфраструктуры Российской Федерации.
Ключевые слова: информационная инфраструктура, информационная безопасность, критически важные объекты инфраструктуры.

ВВЕДЕНИЕ

Рост информационной инфраструктуры, возникающий в общественных отношениях, приводит к тому, что национальная безопасность Российской Федерации имеет существенную зависимость от обеспечения информационной безопасности.

Данная проблема имеет системообразующее значение для развития государства как в политической и экономической сферах, так и для обеспечения безопасности в целом. Приведенное утверждение определяет актуальность проведения научных исследований, направленных на разработку способов и методов обеспечения безопасности информационной инфраструктуры Российской Федерации.

Цель исследования заключается в разработке методических рекомендаций для решения проблемы информационной безопасности КВО Российской Федерации в единой системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на инфраструктуру РФ.

ОСНОВНОЙ МАТЕРИАЛ

Анализ основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, прежде всего, позволяет выделить методы, направленные на оборону КВО.

Данные методы на современном этапе развития государственности способствуют устранению уязвимостей программного обеспечения и разработке

комплексных систем защиты управления критически важных объектов. Кроме того, они предусматривают:

- обнаружение и предупреждение компьютерных атак, создание сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;
- внедрение комплексных систем защиты управления КВО, отвечающих прогрессу информационных технологий и минимизирующих штат обслуживающего персонала [1].

Функционирование КВО инфраструктуры РФ на данном этапе позволяет выделить ряд определенных проблем, которые способствуют нарушению общей безопасности инфраструктуры РФ. Основной проблемой является обеспечение информационной безопасности, которая способствует защите информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении безопасности КВО [2].

Анализ основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, прежде всего, позволяет выделить методы, направленные на оборону КВО.

Данные методы уже на современном этапе развития государственности способствуют устранению уязвимостей программного обеспечения и разработке комплексных систем защиты управления критически важных объектов. Кроме того, они предусматривают:

- обнаружение и предупреждение компьютерных атак, создание сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;
- внедрение комплексных систем защиты управления КВО, отвечающих прогрессу информационных технологий и минимизирующих штат обслуживающего персонала [1].

Функционирование КВО инфраструктуры РФ на данном этапе позволяет выделить ряд определенных проблем, которые способствуют нарушению общей безопасности инфраструктуры РФ. Основной проблемой является обеспечение информационной безопасности, которая способствует защите информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении безопасности КВО [2].

В связи с широкими возможностями использования информационных ресурсов в террористических целях, создаются дополнительные условия возрастания фактора

опасности для личности, социума, государства и их интересов в информационном пространстве.

Информационная безопасность КВО инфраструктуры Российской Федерации – это совокупность систем государственного управления, направленных на обеспечение обороноспособности объектов, нарушение функционирования которых приводит к потере управления и необратимому разрушению инфраструктуры экономики страны, субъекта или административно-территориальной единицы Российской Федерации, снижению безопасности населения государства на длительный период [1].

Как известно, первичная классификации основных источников угроз информационной безопасности предусматривает их деление на внешние и внутренние. Анализ показывает, что наиболее актуальными, в связи со сложившейся ситуацией на международной арене, являются внешние предпосылки, а именно деятельность зарубежных разведывательных и информационных подразделений, направленная против интересов Российской Федерации в информационной сфере через создание условий, предусматривающих ущемление интересов России в мировом информационном пространстве и разработку концепций информационных войн.

К внутренним источникам относятся неблагоприятное состояние отраслей промышленности, тенденция объединения государственных и криминальных структур в информационной сфере, а также снижение степени защищенности конституционных интересов граждан и общества в целом в информационной сфере. Воздействие приведенных угроз на критическую информационную инфраструктуру Российской Федерации может привести к нарушению их функционирования и стать причиной наступления тяжких последствий для государства как в экономической, так и в политической сферах.

Как показывает практический опыт, наибольший вес в современном состоянии защищенности информационного суверенитета России занимают внешние факторы, прежде всего основанные на информационной агрессии и планомерном использовании современных концепций информационных войн. Потому приоритетными в настоящее время являются исследования, направленные на усовершенствование и разработку новых подходов к функционированию системы информационной безопасности инфраструктуры КВО Российской Федерации.

Как указывалось ранее, решение проблематики вопросов безопасности критической информационной инфраструктуры, прежде всего, предусматривает разработку инноваций в отношении комплекса основных способов и методов обеспечения информационной безопасности в целом.

Так, в соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ч. 1, ст. 16), определено, что защита информации представляет собой принятие организационных и правовых мер, которые направлены на обеспечение защиты

информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ информации.

На основании приведенного утверждения целесообразным, по мнению авторов, является разработка инновационного уровневого комплекса мер в составе уровня физической защиты, уровней авторизации и аутентификации, а также уровня поддержки работоспособности (рис. 1):

Рис. 1. Основные способы и методы обеспечения информационной безопасности.

Источник: составлено авторами по материалам [3].

Основываясь на приведенной методологии, возможно создание условий для повышения эффективности системы информационной безопасности инфраструктуры КВО Российской Федерации.

ВЫВОДЫ

Таким образом, используя разработанный механизм информационной безопасности для обеспечения функционирования критической информационной инфраструктуры Российской Федерации, возможно на начальных стадиях защитить

государственный строй от возникновения ситуаций, способных децентрализовать политику и экономику государства. Это, в свою очередь, обеспечивает создание условий политической, экономической и социальной стабильности, искоренение основных угроз в информационном пространстве, приводящих к нарушению международного мира и безопасности, а также обеспечение законности и правопорядка.

Список литературы

1. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012). № 803.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 13.07.2015).

3. Гришина Н. В. Организация комплексной системы защиты информации. М., 2007. С. 250–254.

Статья поступила в редакцию 26.09.2016