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)

(Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803)

I. Общие положения

1. Настоящие Основные направления разработаны в целях реализации основных положений Стратегии национальной безопасности Российской Федерации до 2020 года, в соответствии с которой одним из путей предотвращения угроз информационной безопасности Российской Федерации является совершенствование безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации.

2. Целью государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации является снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства.

3. Основные понятия, используемые в настоящих Основных направлениях:

а) критически важный объект инфраструктуры Российской Федерации (далее - критически важный объект) - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих

территориях, на длительный срок;

б) автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации (далее - автоматизированная система управления КВО) - комплекс аппаратных и программных средств, информационных систем и информационно- телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса критически важного объекта, нарушение (или прекращение) функционирования которых может нанести вред внешнеполитическим интересам Российской Федерации, стать причиной аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизации работы учреждений, предприятий или организаций, нанесения материального ущерба в крупном размере, смерти или нанесения тяжкого вреда здоровью хотя бы одного человека и (или) иных тяжелых последствий (далее - тяжкие последствия);

в) критическая информационная инфраструктура Российской Федерации (далее - критическая информационная инфраструктура) - совокупность автоматизированных систем управления КВО и обеспечивающих их взаимодействие информационно- телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий;

г) компьютерная атака - целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях;

д) безопасность автоматизированной системы управления КВО - состояние автоматизированной системы управления КВО, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения ею целевых функций (далее - штатный режим функционирования) при проведении в отношении ее компьютерных атак;

е) безопасность критической информационной инфраструктуры - состояние элементов критической информационной инфраструктуры и критической информационной инфраструктуры в целом, при котором проведение в отношении ее компьютерных атак не влечет за собой тяжких последствий;

ж) компьютерный инцидент - факт нарушения штатного режима функционирования элемента критической информационной инфраструктуры или критической информационной инфраструктуры в целом;

з) единая государственная система обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов - централизованная, иерархическая, территориально распределенная структура, включающая силы и

средства обнаружения и предупреждения компьютерных атак, а также органы управления различных уровней, в полномочия которых входят вопросы обеспечения безопасности автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры;

и) силы обнаружения и предупреждения компьютерных атак - уполномоченные подразделения федерального органа исполнительной власти в области обеспечения безопасности, федеральных органов исполнительной власти, осуществляющих деятельность в области обеспечения безопасности, государственного надзора и контроля, управления деятельностью критически важных объектов и иных элементов критической информационной инфраструктуры, а также физические лица и специально выделенные сотрудники организаций, осуществляющих эксплуатацию автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры на правах собственности либо на иных законных основаниях, принимающие участие в обнаружении и предупреждении компьютерных атак на критическую информационную инфраструктуру, мониторинге уровня ее реальной защищенности и ликвидации последствий компьютерных инцидентов на основании законодательства Российской Федерации;

к) средства обнаружения и предупреждения компьютерных атак - технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений (ситуационные центры), предназначенные для обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру, мониторинга уровня ее реальной защищенности и ликвидации последствий компьютерных инцидентов;

л) силы ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре - уполномоченные подразделения федерального органа исполнительной власти в области обеспечения безопасности, физические лица и специально выделенные сотрудники организаций, осуществляющих эксплуатацию автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры на правах собственности либо на иных законных основаниях, а также сотрудники предприятий - разработчиков аппаратных средств и программного обеспечения, используемых в автоматизированных системах управления КВО, принимающие на основании законодательства Российской Федерации участие в восстановлении штатного режима функционирования элементов критической информационной инфраструктуры после компьютерных инцидентов;

м) средства ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре - технологии, а также технические, программные, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, предназначенные для восстановления штатного режима функционирования элементов критической информационной инфраструктуры после компьютерных инцидентов.

II. Факторы, влияющие на формирование государственной политики в области

обеспечения безопасности автоматизированных систем управления КВО, и ее основные принципы

4. Обеспечение безопасности автоматизированных систем управления КВО является невозможным без обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом. Данное положение обусловлено повсеместным внедрением широкого спектра информационных технологий в системы управления производственными и технологическими процессами КВО, глобализацией современных информационно-телекоммуникационных сетей, превращением их в единую мировую информационно-телекоммуникационную сеть с размытыми границами национальных сегментов, существенным увеличением доли распределенных автоматизированных систем управления КВО и все большим использованием информационно-телекоммуникационных сетей и сетей связи общего использования для их информационного обмена.

5. Факторы, влияющие на формирование государственной политики в области обеспечения безопасности автоматизированных систем управления КВО:

а) интеграция в единые комплексы автоматизированных систем управления КВО и других информационных систем, используемых в управлении производственными и транспортными структурами, административными и финансовыми ресурсами;

б) постоянное усложнение используемых в автоматизированных системах управления КВО программного обеспечения и оборудования;

в) практика осуществления иностранными фирмами технического обслуживания и удаленной настройки автоматизированных систем управления КВО в целом или их составных частей, а также телекоммуникационного оборудования, входящего в состав критической информационной инфраструктуры;

г) стремление организаций - разработчиков программного обеспечения автоматизированных систем управления КВО к снижению издержек и, как следствие, использованию типовых решений и заимствованного программного обеспечения;

д) интенсивное совершенствование средств и методов использования информационных и коммуникационных технологий для нанесения ущерба Российской Федерации, а также участившиеся попытки их применения в противоправных целях и конкурентной борьбе;

е) усиление угрозы терроризма, рост числа противоправных деяний с использованием информационных и коммуникационных технологий;

ж) сложившаяся среди операторов и владельцев информационных систем, в состав которых входят автоматизированные системы управления КВО, тенденция сокрытия попыток или фактов нарушения их штатного функционирования;

з) недостаточный уровень образования и профессиональной подготовки персонала, обслуживающего автоматизированные системы управления КВО, снижение технологической культуры производства;

и) отсутствие достаточного нормативно-правового регулирования процессов обеспечения безопасности автоматизированных систем управления КВО, в том числе в части определения уровня их реальной защищенности;

к) вынужденное привлечение при создании автоматизированных систем управления КВО иностранных фирм - производителей и поставщиков программно-аппаратных средств обработки, хранения и передачи информации и применение зарубежных программно- аппаратных решений, создающих предпосылки для возникновения технологической и иной зависимости от иностранных государств.

6. Основные принципы государственной политики в области обеспечения безопасности автоматизированных систем управления КВО:

а) соблюдение законодательства Российской Федерации, а также требований международных договоров Российской Федерации всеми участниками процесса создания и эксплуатации автоматизированных систем управления КВО;

б) сочетание интересов и взаимной ответственности государства, граждан, а также организаций, участвующих в разработке, создании и эксплуатации автоматизированных систем управления КВО;

в) персонификация ответственности должностных лиц, операторов, персонала и иных лиц, принимающих участие в разработке, создании, вводе в действие, эксплуатации и модернизации автоматизированных систем управления КВО;

г) обеспечение комплексной защиты критической информационной инфраструктуры в целом, включая создание единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов;

д) обеспечение разрешительного характера деятельности в области обеспечения безопасности автоматизированных систем управления КВО с использованием механизмов лицензирования и сертификации;

е) разделение функций между федеральным органом исполнительной власти в области обеспечения безопасности и иными федеральными органами исполнительной власти, осуществляющими деятельность в области безопасности, органами государственного надзора и контроля, управления деятельностью критически важных объектов и иных элементов критической информационной инфраструктуры, усиление координации их деятельности;

ж) регламентация прав и обязанностей собственников автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, а также эксплуатирующих их организаций;

з) недопущение технологической или иной зависимости от иностранных государств при осуществлении деятельности в области обеспечения безопасности автоматизированных систем управления КВО.

III. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления КВО

7. Решение основных задач государственной политики в области обеспечения безопасности автоматизированных систем управления КВО должно осуществляться по следующим направлениям:

а) совершенствование нормативно-правовой базы;

б) государственное регулирование;

в) промышленная и научно-техническая политика;

г) фундаментальная и прикладная наука, технологии и средства обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры;

д) повышение квалификации кадров в области обеспечения безопасности автоматизированных систем управления КВО.

8.Основные задачи, касающиеся совершенствования нормативно-правовой базы в области обеспечения безопасности автоматизированных систем управления КВО:

а) определение и разграничение полномочий федерального органа исполнительной власти в области обеспечения безопасности, иных федеральных органов исполнительной власти, осуществляющих деятельность в области обеспечения безопасности, органов государственного надзора и контроля, управления деятельностью критически важных объектов и иных элементов критической информационной инфраструктуры;

б) законодательное определение и закрепление прав и обязанностей собственников автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры и эксплуатирующих их организаций. в области обеспечения безопасности автоматизированных систем

управления КВО;

в) определение порядка:

разработки, ввода в действие, эксплуатации и модернизации автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры;

получения федеральным органом исполнительной власти в области обеспечения безопасности информации об автоматизированных системах управления КВО и иных элементах критической информационной инфраструктуры;

использования сил и средств обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру;

использования сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;

действий должностных лиц, персонала и владельцев автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры при обнаружении попыток или фактов нарушения штатного функционирования этих объектов в случае компьютерных инцидентов;

г) создание правовых оснований и определение порядка применения мер принудительного изменения информационного обмена с объектами информатизации, являющимися источниками компьютерных атак, вплоть до его полного прекращения;

д) нормативно-правовое обеспечение функционирования единой государственной системы обнаружения компьютерных атак на критическую информационную инфраструктуру и мониторинга уровня ее реальной защищенности;

е) введение ответственности за нарушение порядка разработки, ввода в действие, эксплуатации и модернизации автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры;

ж) усиление ответственности за создание и (или) применение средств компьютерных атак;

з) оптимизация законодательства Российской Федерации в части лицензирования деятельности, связаннойс разработкой, производством, эксплуатацией и техническим обслуживанием автоматизированных систем управления критически важными объектами.

9. Основные задачи государственного регулирования в области обеспечения безопасности автоматизированных систем управления КВО:

а) развитие механизмов государственного управления и контроля, а также усиление координации в области обеспечения безопасности критической информационной инфраструктуры;

б) выделение (привлечение) необходимых объемов и источников финансовых ресурсов (бюджетных и внебюджетных) на реализацию программ и планов мероприятий в области обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом;в) создание единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки защищенности ее элементов;

г) обеспечение устойчивого функционирования национального сегмента единой мировой информационно-телекоммуникационной сети в условиях массированного деструктивного информационного воздействия с территорий, находящихся вне юрисдикции Российской Федерации;

д) создание условий, стимулирующих развитие на территории Российской Федерации производства телекоммуникационного оборудования, устойчивого к компьютерным атакам;

е) создание и поддержание в постоянной готовности сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;

ж) развитие международного сотрудничества, включая совершенствование международной кооперации в области обеспечения информационной безопасности;

з) стимулирование, в том числе материальное, проведения частными организациями и лицами исследований в области обнаружения уязвимостей программного обеспечения и оборудования, применяемого в автоматизированных системах управления КВО и на иных объектах критической информационной инфраструктуры, с представлением результатов федеральному органу исполнительной власти в области обеспечения безопасности.

10. Основные задачи по совершенствованию промышленной и научно-технической политики в области, обеспечения безопасности автоматизированных систем управления КВО:

а) проведение комплекса мероприятий по развитию систем, средств и методов технической оценки уровня реальной защищенности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом;

б) создание единых реестров программных и аппаратных средств, используемых в автоматизированных системах управления КВО, создание баз данных, касающихся надежности функционирования автоматизированных систем управления КВО, состояния их защищенности, состояния технического оборудования, оценки эффективности действующих и внедряемых на критически важных объектах мер безопасности;

в) проведение комплекса организационно-технических мероприятий по исключению прохождения информационного обмена автоматизированных систем управления КВО по территориям иностранных

государств, а при технической невозможности такого исключения - создание и применение защитных мер, обеспечивающих отсутствие любых негативных воздействий на процессы, контролируемые автоматизированными системами управления КВО, в случае нарушения штатного функционирования этого канала связи;

г) разработка комплекса мер по созданию и внедрению телекоммуникационного оборудования, устойчивого к компьютерным атакам;

д) создание хранилища эталонного программного обеспечения, используемого в автоматизированных системах управления КВО и на других объектах критической информационной инфраструктуры;

е) развитие (с учетом мобилизационной готовности) научно- производственной базы, обеспечивающей выпуск систем (средств) обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры;

ж) разработка и внедрение импортозамещающих технологий, материалов, комплектующих и других видов продукции, используемых в автоматизированных системах управления КВО.

11. Основные задачи в области развития фундаментальной и прикладной науки, технологий и средств обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры:

а) разработка методов и средств своевременного выявления угроз и оценки их опасности для автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры;

б) разработка и внедрение специализированных информационно-аналитических систем, развитие исследований в области математического моделирования процессов обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, направленных на выработку вероятных сценариев развития ситуации и поддержку управленческих решений;

в) разработка и внедрение комплексных систем защиты и обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, отвечающих современному уровню развития информационных технологий и минимизирующих участие обслуживающего персонала в настройке и эксплуатации входящих в их состав программно-аппаратных средств;

г) разработка для автоматизированных систем управления КВО специализированных экономически целесообразныхинформационных технологий, исключающих или в максимальной степени снижающих на технологическом уровне обмен информацией, подлежащей обязательной защите.

12. Основные задачи по совершенствованию образования, подготовки и повышения квалификации

кадров в области обеспечения безопасности автоматизированных систем управления КВО, повышению общего уровня культуры информационной безопасности граждан:

а) совершенствование системы подготовки, переподготовки и аттестации кадров (в том числе руководящих) в области обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры на базе профильных образовательных учреждений;

б) повышение общего уровня культуры информационной безопасности граждан, включая повышение информированности населения о критической информационной инфраструктуре, угрозах информационной безопасности и способах защиты от этих угроз;

в) формирование в общественном сознании нетерпимости к лицам, совершающим противоправные деяния с использованием информационных технологий.

IV. Основные механизмы и этапы реализации государственной политики в области обеспечения безопасности автоматизированныхсистем управления КВО

13. Реализация настоящих Основных направлений обеспечивается путем консолидации усилий органов государственной власти и институтов гражданского общества, направленных на защиту интересов Российской Федерации посредством комплексного использования правовых, организационных, технических, социально- экономических, специальных и иных мер поддержки.

14. Координацию деятельности федеральных органов исполнительной власти по реализации настоящих Основных направлений осуществляет федеральный орган исполнительной власти в области обеспечения безопасности.

15. Настоящие Основные направления реализуются в рамках:

а) существующих и планируемых государственных программ;

б) плана мероприятий по реализации настоящих Основных направлений, утверждаемого Правительством Российской Федерации.

16. Настоящие Основные направления реализуются поэтапно.

17. На первом этапе (2012 - 2013 годы) необходимо осуществить:

а) подготовку плана мероприятий по реализации настоящих Основных направлений;

б) нормативно-правовое определение и разграничение полномочий и ответственности федерального органа исполнительной власти в области обеспечения безопасности, иных федеральных органов исполнительной власти, осуществляющих деятельность в области обеспечения безопасности, органов государственного надзора и контроля, управления деятельностью КВО и объектов критической информационной инфраструктуры;

в) определение порядка использования сил и средств обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру;

г) разработку концепции использования сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;

д) определение необходимых объемов и источников финансовых ресурсов (бюджетных и внебюджетных) на реализацию программ и планов мероприятий в области обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом на период второго этапа реализации настоящих Основных направлений;

е) подготовку предложений по внесению изменений в утвержденные государственные программы и корректировке планируемых государственных программ.

18. На втором этапе (2014 - 2016 годы) необходимо осуществить:

а) разработку нормативных правовых актов, определяющих:

порядок получения федеральным органом исполнительной власти в области обеспечения безопасности информации об автоматизированных системах управления КВО и иных объектах критической информационной инфраструктуры;

права и обязанности собственников автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, а также эксплуатирующих их организаций в области обеспечения их безопасности;порядок разработки, ввода в действие, эксплуатации и модернизации автоматизированных систем управления КВО;

регламент функционирования единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки защищенности ее элементов;

порядок ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;

действия должностных лиц, персонала и владельцев автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры при обнаружении несанкционированного доступа к обрабатываемой информации и иных компьютерных инцидентах;

ответственность за нарушение установленного порядка разработки, ввода в действие, эксплуатации и модернизации автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры;

правовые основания и порядок применения мер принудительного изменения информационного обмена с объектами информатизации, являющимися источниками компьютерных атак, вплоть до полного его прекращения;

б) проведение паспортизации автоматизированных систем управления КВО;

в) реализацию первоочередных мероприятий, направленных на минимизацию прохождения информационного обмена между российскими абонентами по территориям иностранных государств;

г) разработку системы грантов для частных лиц и организаций, призванных стимулировать исследования в области обнаружения уязвимостей программного обеспечения и оборудования автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры;

д) разработку комплексных систем защиты и обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, отвечающих современному уровню развития информационных и коммуникационных технологий и минимизирующих участие обслуживающего персонала в настройке и эксплуатации входящих в их состав программно-аппаратных средств;

е) определение необходимых объемов и источников финансовых ресурсов (бюджетных и внебюджетных) на реализацию программ и планов мероприятий в области обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом на последующих этапах реализации настоящих Основных направлений;

ж) ввод в эксплуатацию первой очереди Ситуационного центра единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов;

з) создание сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре.

19. На третьем этапе (2017 - 2020 годы) необходимо осуществить:

а) внедрение комплексных систем защиты и обеспечения безопасности автоматизированных систем

управления КВО и иных объектов критической информационной инфраструктуры, отвечающих современному уровню развития информационных технологий и минимизирующих участие обслуживающего персонала в настройке и эксплуатации входящих в их состав программно- аппаратных средств;

б) реализацию комплекса организационных, правовых, экономических и научно-технических мер по прекращению прохождения информационного обмена между российскими абонентами по территориям иностранных государств;в) ввод в действие первой очереди хранилища эталонного программного обеспечения, используемого в автоматизированных системах управления КВО и на других объектах критической информационной инфраструктуры;

г) внедрение системы грантов для частных лиц и организаций для стимулирования исследований в области обнаружения уязвимостей программного обеспечения и оборудования автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры;

д) ввод в эксплуатацию Ситуационного центра единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру Российской Федерации и оценки уровня реальной защищенности ее элементов и ситуационных центров регионального и ведомственного уровней;

е) создание для автоматизированных систем управления КВО специализированных экономическицелесообразных информационных технологий, исключающих или в максимальной степени снижающих на технологическом уровне обмен информацией, подлежащей обязательной защите;

ж) ввод в эксплуатацию в целом единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов.

20. В период после 2020 года осуществляется комплекс мероприятий по поддержанию организационной, экономической, научно-технической и технологической готовности Российской Федерации к предотвращению угроз безопасности ее критической информационной инфраструктуры.