Систематизация основ методологии синтеза критической информационной инфраструктуры Российской Федерации

Полковник О.М. ЛЕПЕШКИН,
доктор технических наук

Майор О.А. ОСТРОУМОВ,
кандидат технических наук

Полковник запаса А.Д. СИНЮК,
доктор технических наук

АННОТАЦИЯ

Введены понятия критичности систем связи и управления. Показана необходимость разработки подходов к систематизации методологии синтеза критической информационной инфраструктуры и критически важных объектов систем связи и управления.

КЛЮЧЕВЫЕ СЛОВА

Критическая информационная инфраструктура, критически важный объект, безопасность информации, функциональная устойчивость, система управления, система связи.

ABSTRACT

The paper introduces the concepts of critical nature of communication and control systems. It shows the need to develop approaches to systematizing the methodology of synthesizing the critical information infrastructure and crucial facilities of communication and control systems.

KEYWORDS

Critical information infrastructure, critically important facility, information security, functional stability, control system, communication system.

В СОВРЕМЕННЫХ условиях вопросу обеспечения безопасности уделяется много внимания, причем с каждым годом особенно в сфере информационных технологий он часто становится одним из главных.

Развитие общества, его информатизация, возможность доступа к информации в любых условиях нами понимается как должное. Обращаясь к информации, мы думаем, что она защищена. И если информация отдельного гражданина (если он не крупный руководитель, политик и т. д.) скорее всего заинтересует небольшой круг лиц, то информация о крупных предприятиях, ведомствах государства, их контрактах, сделках, об их руководстве и т. д. интересует многих, особенно это касается силового сектора государства и связанных с ним отраслей промышленности. Объекты интереса нарушителей при различном воздействии на них могут повести себя по-разному: от простого игнорирования их до целенаправленных действий, направленных на предприятие, ведомство,

министерство и т.д. или их части, вследствие чего может быть выведен из строя объект (нарушено его функционирование, управление). Все это может привести к финансовым, материальным и людским потерям, что, несомненно, должно учитываться в военном деле.

В Федеральном законе от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» представлено понятие «критически важный объект» (КВО) как объект, нарушение (или прекращение) функционирования которого приводит к потере управления экономикой РФ, субъекта РФ или административно-территориальной единицы субъекта РФ, ее необратимому негативному изменению (или разрушению) либо существенному снижению безопасности жизнедеятельности населения.

В «Основных направлениях 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) вводится понятие КВО АСУ.

В июле 2017 года был принят ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации», определены субъекты и объекты критической информационной инфраструктуры (КИИ). Объектами являются информационные системы (ИС), информационно-телекоммуникационные сети (ИТКС), автоматизированные системы управления (АСУ) субъектов КИИ, кроме этого к КИИ относят сети электросвязи (СЭС), используемые для организации взаимодействия таких объектов. Субъектами — государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в различных сферах жизни общества, а также российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей. Данным законом определены общие субъекты и объекты КИИ, а руководители министерств и ведомств определяют критичность своих объектов и субъектов и подают заявки на внесение их в государственный реестр объектов КИИ. Для обеспечения разделения (ранжирования) объектов МО РФ необходим соответствующий методологический подход, который в явном виде на данный момент отсутствует.

Работы по обеспечению безопасности критически важных объектов можно разделить на два этапа: до выхода Федерального закона № 187 и после его выхода. В законе четко определились с объектами КИИ, защита которых имеет первостепенное значение, и основной угрозой — компьютерными атаками (КА). Одним из элементов КИИ является сеть электросвязи, обеспечивающая взаимодействие остальных объектов КИИ, которая является составной частью системы связи.

Современная система связи (СС) — это огромный организм, состоящий из подсистем в регионах, отдельных городах и населенных пунктах. Аналогично система связи специального назначения также является сложным образованием, состоящим из различных систем, сетей, подсистем, объектов и являющимся составной частью системы управления (СУ). Выход

системы связи из строя приведет к срыву управления войсками и оружием, что может привести к людским потерям, потерям в технике, провалу операции или всей кампании. Выход из строя отдельных средств, элементов системы связи может привести к нарушению функционирования самой системы, что приведет (может привести) к нарушению управления. В этом случае можно говорить о высокой важности или критичности этих элементов для систем связи и управления, а системы связи для системы управления и процесса управления.

Рассматривая сеть электросвязи специального назначения как объект КИИ, подверженный компьютерным атакам и предназначенный для взаимодействия АСУ, ИС и ИТКС, необходимо учитывать, что через любой элемент системы можно осуществить воздействие на другой ее элемент, в частности на сеть электросвязи. Кроме этого, система связи как элемент системы управления является КВО для системы управления. В свою очередь, система управления будет критически важной для процесса управления.

Под критичностью управления понимается состояние управления быть подвергнутым воздействию дестабилизирующих факторов, вследствие которых происходит нарушение (или прекращение) устойчивого управления объектом, т. е. невозможность объектом выполнять возложенные на него задачи (выполнение своего функционала).

Под критически важной системой связи специального назначения можно понимать часть системы управления, нарушение (или прекращение) устойчивого функционирования которой приводит к нарушению (или прекращению) устойчивого функционирования системы управления, потере управления, разрушению инфраструктуры, зависящей от данной СУ, 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.

Под критически важной системой управления специального назначения можно понимать такую систему, нарушение (или прекращение) устойчивого функционирования которой приводит к нарушению (или прекращению) управления, разрушению инфраструктуры, зависящей от данной СУ, 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.

Под критической информационной инфраструктурой системы связи специального назначения можно понимать часть системы связи, воздействие на которую КА приводит (может привести) к нарушению (или

Современная система связи — это огромный организм, состоящий из подсистем в регионах, отдельных городах и населенных пунктах. Аналогично система связи специального назначения также является сложным образованием, состоящим из различных систем, сетей, подсистем, объектов и являющимся составной частью системы управления. Выход системы связи из строя приведет к срыву управления войсками и оружием.

прекращению) устойчивого функционирования системы связи, потере управления, разрушению инфраструктуры, зависящей от данной СУ, 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.

Под критической информационной инфраструктурой системы управления специального назначения можно понимать часть системы управления, воздействие на которую КА приводит (может привести) к нарушению (или прекращению) устойчивого функционирования системы управления, потере управления, разрушению инфраструктуры, зависящей от данной СУ, 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.

Под критически важным объектом критической СС — часть системы связи, нарушение (или прекращение) устойчивого функционирования которой приводит к нарушению (или прекращению) устойчивого функционирования системы связи, системы управления, потере управления, разрушению инфраструктуры, зависящей от данной СУ, 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.

Под критически важным объектом критической СУ — часть системы управления, нарушение (или прекращение) устойчивого функционирования которой приводит к нарушению (или прекращению) устойчивого функционирования системы управления, потере управления, разрушению инфраструктуры, зависящей от данной СУ, 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.

Под функциональной устойчивостью системы связи понимается способность системы связи выполнять возложенные на нее функции по предоставлению всех видов услуг должностным лицам, осуществляющим управление в условиях воздействия на нее различных дестабилизирующих факторов в установленные сроки с заданным качеством.

Развитие техники и средств передачи информации позволило пользователям получать большее количество услуг, однако стоимость такой связи возросла значительно. В современных условиях дешевле арендовать инфраструктуру различных операторов, например, Ростелекома. При этом с большой долей вероятности можно говорить об отсутствии доступа к сети и ее ресурсам только на участке, который находится под вашим контролем, а участок арендодателя является «черным ящиком». С какой долей вероятности противник получает доступ к оборудованию арендодателя, мы не знаем. Кроме того, оборудование сторонней организации становится критичным для системы связи специального назначения.

Вместе с развитием и совершенствованием техники, предназначен-

ной для передачи информации, происходит развитие средств воздействия на элементы системы связи. При этом такое воздействие может привести к сбоям в работе оборудования или его поломке, что в определенный момент, когда необходимо передать информацию, может привести к пагубным последствия, к смерти личного состава и мирного населения.

Одними из самых опасных современных угроз для сетей связи являются компьютерные атаки, которые представляют собой не единичное действие, а, как правило, сложный комплекс мероприятий, включающий подготовку, разведку, поиск уязвимостей и т. д., направленных на получение контроля над ресурсом, взлома, заражения системы, нарушения ее функционирования. Для КВО инфраструктуры системы связи вероятность возникновения подобных воздействий должна быть минимизирована. Государственные и частные организации, как правило, имеют определенный набор средств обеспечения безопасности информации, однако, как показывает практика, эти средства не всегда позволяют противодействовать воздействию сторонних лиц. Возникает необходимость построения динамичной во времени современной системы безопасности объектов КИИ, позволяющей не только обеспечивать противодействие совершаемым воздействиям, но и осуществлять поиск уязвимостей, выявлять оборудование, работающее со сбоями, прогнозировать места воздействия противника, отключать от сети без потери функциональных возможностей все системы, оборудование, на которое осуществляется воздействие. Исследованию этого вопроса необходимо уделять внимание.

Под критически важным объектом критической СУ — часть системы управления, нарушение устойчивого функционирования которой приводит к нарушению устойчивого функционирования системы управления, потере управления, разрушению инфраструктуры, зависящей от данной СУ, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно-территориальной единицы.

Анализ работ, посвященных исследованию КИИ, позволяет сделать вывод об отсутствии взаимосвязанной структурированной методологии синтеза КИИ, ее элементов, а также КВО системы управления. Авторы рассматривают отдельные объекты КИИ, при этом больше всего внимания уделяется автоматизированным системам управления[1—7]. В меньшей степени рассмотрены ИС и ИТКС[8,9]. Связующим элементом между АСУ, ИС и ИТКС является система связи, с помощью которой осуществляется их взаимодействие, которое также подвержено КА[10,11]. Вопросам оценки критичности системы связи для системы управления и системы управления для управления уделяется мало внимания.

Кроме этого, возникает противоречие в практике, обусловленное наличием требований к КИИ, вводимым ФЗ № 187, и фактически отсутствующей системой обеспечения безопасности КИИ с учетом требований к критичности.

Интерес к вопросу обеспечения безопасности, устойчивости, функциональной устойчивости КВО, КИИ большой. В рамках рассмотренных в статье вопросов решаются научные задачи обеспечения оценки состояния системы безопасности или устойчивости объектов КИИ от воздействия компьютерных атак (деструктивных информационных воздействий). Вопросы разработки

методологии или концепции обеспечения функциональной устойчивости объектов КИИ, указанных в ФЗ № 187 от 26.07.2017 года, в полной мере не рассматриваются. Кроме этого, не уделяется внимания понятию критичности важного объекта специального назначения, что определяет необходимость разработки методологического и методического подходов определения критичности объектов Министерства обороны РФ. В законе определена КИИ, которая включает объекты КИИ и сети электросвязи, предназначенные для взаимодействия объектов. В связи с этим необходимо актуализировать внимание к проблеме критичности СС специального назначения для системы управления, а СУ для процесса управления. Для обеспечения устойчивого функционирования критических объектов и своевременного реагирования при выходе из строя отдельных элементов или в целом объекта, а также принятия мер к решению таких ситуаций требуется разработка методологического подхода, методического и математического аппарата, описывающих критичность СС, СУ, а также органа (органов) контроля за состоянием СС, СУ, их объектов и элементов.

ПРИМЕЧАНИЯ

[1] *Скрыпник А.В.* Методический аппарат ранжирования критически важных объектов противника в целях решения задачи силового стратегического сдерживания // Труды молодых ученых Вооружение и экономика. 2011. № 3 (15). С. 129—140.

[2] *Лепешкин О.М., Гаппоев Р.С.* Оптимизация структуры комплекса технических средств в информационно-управляющих системах государственного управления // Научно-технические ведомости СпбГПУ. 2011. № 5. С. 129—132.

[3] *Павлов А.Н., Павлов Д.А.* Подход к прогнозированию структурной устойчивости сложных объектов // Автоматизированные системы управления. 2013. № 6. С. 64—66.

[4] *Калашников А.О.* Управление информационными рисками объектов критической информационной инфраструктуры РФ // Вопросы кибербезопасности. 2014. № 3. С. 35—41.

[5] *Куделькина В.А., Янникова И.М.* Структурная схема интеллектуальной интегрированной системы безопасности критически важных и потенциально опасных объектов // Известия Самарского научного центра Российской академии наук. 2015. Т. 17. № 6. С. 570—572

[6] *Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г.* Кибербезопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4. С. 2—10.

[7] *Климов С.М.* Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки. 2016. № 8. С. 27—35.

[8] *Дурнев Р.Ф., Мещеряков Е.М.* Повышение устойчивости функционирования критически важных объектов при воздействии современных средств поражения: перспективные задачи гражданской обороны // Технологии гражданской безопасности. 2016. Т. 13. № 2 (48). С. 54—58.

[9] *Дроботун Е.Б.* Построение модели угроз безопасности информации в АСУ КВО на основе сценариев действия нарушителя // Программные продукты и системы. 2016. Т. 29. № 3. С. 42—50.

[10] *Олейник А.С.* Методы оценки эффективности защиты критически важных объектов // Вестник Московского университета МВД России. 2017. № 4. С. 280—286.

[11] *Прохоров М.А.* Модель оценивания устойчивости автоматизированных систем управления КВО в условиях деструктивных воздействий // Известия ТулГУ. Технические науки. 2018. № 6. С. 220—228.