УДК 681.3

**О.С. Авсентьев, А.Н. Бабкин, С.А. Бабкин**

# Организационно-техническое и правовое обеспечение безопасности инфокоммуникационных систем объектов «критической инфраструктуры» в Российской Федерации

Рассматриваются вопросы обеспечения информационной безопасности объектов «критической инфраструктуры» в Российской Федерации. К подобным объектам относятся объекты электроснабжения, теплоснабжения, связи и телекоммуникаций, транспортной инфраструктуры, правоохранительной системы и др. Представлена обобщенная модель ключевой системы информационной инфраструктуры.

**Ключевые слова**: информационная безопасность, объект критической инфраструктуры, защита информации, автоматизированная система управления, инфокоммуникационная система.

Результатом научно-технического прогресса последних десятилетий, определившим основное направление мирового развития, является широкое применение инфокоммуникационных систем (ИКС) и технологий для повышения эффективности функционирования основных государственных структур и их объектов «критической инфраструктуры».

В соответствии с основными руководящими документами ФСТЭК России под «критически важным объектом» понимается объект, оказывающий существенное влияние на национальную безопасность Российской Федерации. Прекращение или нарушение функционирования такого объекта приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики или другой сферы деятельности страны.

Территориальная распределенность элементов ИКС «критически важного объекта» обусловливает жесткие требования к оперативности принятия управленческих решений по обеспечению безопасности его функционирования.

Это особо актуально для объектов, функционирование которых тесно связано с соответствующими муниципальными объектами, что в значительной степени усложняет проведение мероприятий организационно-технического и правового обеспечения безопасности их ИКС в условиях воздействия различного рода негативных факторов.

Одним из наиболее существенных факторов снижения эффективности ИКС объектов «критической инфраструктуры» являются угрозы нарушения информационной безопасности.

В соответствии с Доктриной информационной безопасности Российской Федерации [1] одной из важнейших составляющих ее национальных интересов в информационной сфере считается «… защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России».

Решение данной задачи должно осуществляться системно, на основе всестороннего исследования как информационных процессов, реализуемых в ИКС рассматриваемого типа, так и механизмов реализации угроз их информационной безопасности и технологий защиты информации. То обстоятельство, что подобные процессы, механизмы и технологии реализуются с использованием средств, характеризующихся множеством разнородных параметров, относит вопросы организационно-технического и правового обеспечения безопасности информации объектов «критической инфраструктуры» к числу сложных как в методическом, так и в практическом плане.

Это требует разработки нового подхода к синтезу систем защиты информации (СЗИ) и оценке их эффективности на объектах «критической инфраструктуры» в условиях воздействия угроз информационной безопасности. Суть этого подхода должна состоять в разработке методов и алгоритмов формирования СЗИ и аппарата системной оценки защищенности ИКС.

В процессе реализации данного подхода целесообразно выделить следующие задачи:

– определение перечня объектов, функционирование которых существенно зависит от состояния безопасности информационной инфраструктуры (определение объекта защиты). При этом с це-

лью достижения необходимого и достаточного уровня защищенности информации, циркулирующей в ИКС объектов «критической инфраструктуры», целесообразно определение ее ценности (степени конфиденциальности);

– выявление возможных угроз, связанных с функционированием ИКС этих объектов;

– оценка существующего нормативного и правового обеспечения защиты объектов «критической инфраструктуры» от несанкционированного доступа в их ИКС и формулировка предложений по их совершенствованию;

– проработка организационно-технических и правовых вопросов защиты этих объектов от целенаправленных противоправных воздействий на их ИКС;

– определение перечня субъектов, которые должны участвовать в обеспечении информационной безопасности данных объектов, с анализом их возможностей и готовности принять участие в работе.

Соответственно, информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), считается ключевой (критически важной) системой информационной инфраструктуры (КСИИ).

В этом случае обрабатываемая в КСИИ информация о состоянии критически важного объекта (процесса), информация о КСИИ (о ее составе, характеристиках программного и программно-аппаратного обеспечения, размещении, коммуникациях и др.), которая в случае ее хищения (ознакомления с ней) может быть непосредственно использована для деструктивных информационных воздействий, а также иная информация, уничтожение, блокирование или искажение которой может привести к нарушению функционирования КСИИ, является критически важной.

Под обеспечением безопасности информации в ключевых системах информационной инфраструктуры понимается деятельность, направленная на ликвидацию угроз или на минимизацию ущерба от реализации угроз безопасности информации в ключевых системах информационной инфраструктуры.

В соответствии с приведенной выше терминологией в качестве ИКС объекта «критической инфраструктуры» Российской Федерации будем понимать КСИИ как инфокоммуникационную систему, которая осуществляет управление критически важным объектом (процессом) и (или) информационное обеспечение управления таким объектом (процессом), или официальное информирование общества (граждан), в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация и (или) будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

Типовая обобщенная модель КСИИ, осуществляющая управление критически важным объектом (процессом), представлена на рис. 1 и включает следующие основные компоненты:

– управляющую подсистему;

– информационно-измерительную подсистему (контроля, регистрации);

– информационно-исполнительную подсистему;

– подсистему внешнего управления и контроля.

Центральным звеном КСИИ является управляющая подсистема, которая предназначена для выполнения следующих основных задач:

– анализ актуальных данных об управляемом (контролируемом) критически важном объекте (процессе);

– анализ управляющей информации от внешних управляющих объектов (административной подсистемы);

– принятие (на основе результатов анализа) решений по управлению критически важным объектом (процессом) или компонентами;

– генерация команд управления критически важным объектом (процессом) или компонентами КСИИ.

Информационно-измерительная подсистема предназначена для выполнения следующих основных задач:

– формирование информационных сообщений о параметрах (состоянии) управляемого критически важного объекта (процесса) с использованием соответствующих датчиков (средств измерения, контроля);

– сбор и передача информации о параметрах (состоянии) управляемого критически важного объекта (процесса) от датчиков в управляющую подсистем) с использованием соответствующих средств связи и передачи данных.

Информационно-исполнительная подсистема отвечает за передачу (или) интерпретацию управляющей информации (команд управления) от управляющей подсистемы к исполнительным средствам и системам, оказывающим соответствующее воздействие на управляемый критически важный объект (процесс).

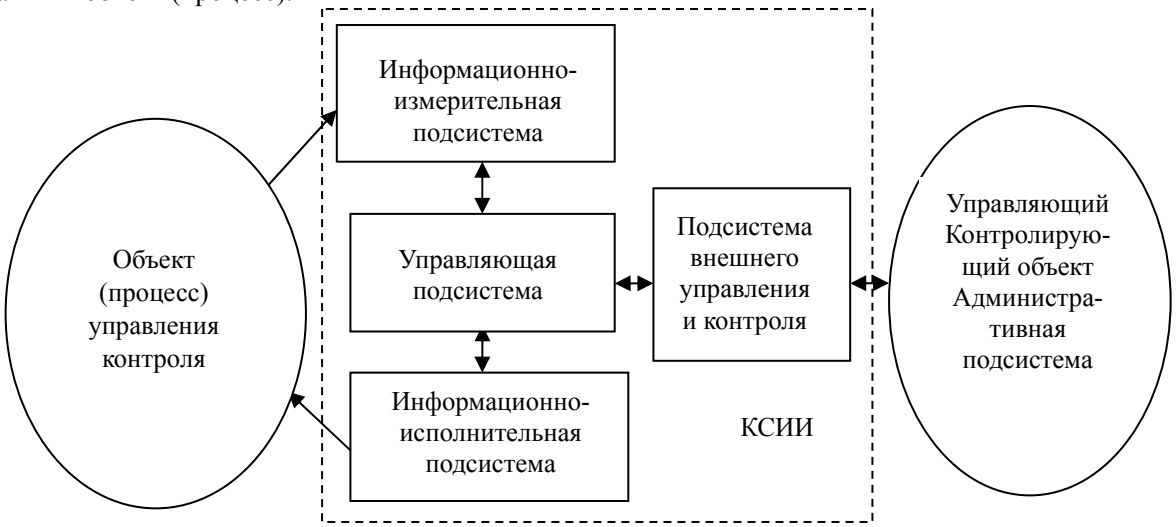


Рис. 1. Структурная схема ключевой системы информационной инфраструктуры

Подсистема внешнего управления и контроля обеспечивает взаимодействие управляющей подсистемы с внешним управляющим (контролирующим) объектом (процессом), осуществляющим администрирование КСИИ, и предназначена для выполнения следующих основных задач:

– сбор и передача управляющей подсистеме команд управления с внешних управляющих (контролирующих) объектов (процессов);

– передача статусной информации о состоянии КСИИ (ее компонентов) и (или) управляемого (контролируемого) критически важного объекта (процесса) от управляющей подсистемы внешним управляющим (контролирующим) объектам (процессам).

Подсистема внешнего управления может представлять собой автоматизированную систему (АС) «офисного типа» и (или) специализированные диспетчерские рабочие места.

В состав информационно-измерительной, информационно-исполнительной подсистем, а также подсистемы внешнего управления входит подсистема передачи данных, отвечающая за транспортировку всей циркулирующей в КСИИ информации. Эта подсистема включает средства, формирующие различные каналы передачи данных (проводные, оптоволоконные, радиоканалы и др.), а также средства, обеспечивающие интерфейс подсистемы передачи данных с основными подсистемами КСИИ.

Такие системы развернуты и функционируют в критически важных сегментах информационной инфраструктуры страны и включают [1, 2]:

- системы органов государственной власти;
- системы органов управления правоохранительных структур;
- системы финансово-кредитной и банковской деятельности;
- системы предупреждения и ликвидации чрезвычайных ситуаций;
- географические и навигационные системы;
- сети связи общего пользования на участках, не имеющих резервных или альтернативных видов связи;
- системы специального назначения;
- спутниковые системы, используемые для обеспечения органов управления и в специальных целях;
- системы управления добычей и транспортировкой нефти, нефтепродуктов и газа;
- системы управления водоснабжением;
- системы управления энергоснабжением;
- системы управления транспортом (наземным, воздушным, морским);

– системы управления потенциально опасными объектами;

– системы, которые не относятся к вышеуказанным, но нарушение штатного режима функционирования которых может привести к нарушению функций управления чувствительными для Российской Федерации процессами.

Как КСИИ, так и их элементы, а также обрабатываемая в них информация являются объектом воздействия различного рода угроз, а следовательно, и объектом защиты.

Указанные обстоятельства позволяют отнести КСИИ к сложным системам [4]. Используя аппарат теории множеств, определим их соответствия и композиции [3].

В качестве области отправления соответствия $\{O\}$ определим множество закономерностей функционирования КСИИ, ее демаскирующих признаков, каналов утечки информации, а в качестве области прибытия соответствия $\{П\}$ – множество закономерностей возникновения угроз, функционирования технических разведок (ТР), их возможностей по добыванию информации, циркулирующей в КСИИ, и сведений о ней.

Указанные соответствия представляются в виде композиции с областей интересов ТР к КСИИ в виде

$$c = (O, П, C), \tag{1}$$

где $O$ – совокупность элементов, сопоставляемых с элементами $П$; $П$ – совокупность элементов, сопоставляемых с элементами $O$; $\{C \subset O \times П\}$ – множество, устанавливающее закон определения $c$, представляющий перечисление всех пар $(o, n)$, участвующих в сопоставлении.

При этом допускается сопоставление ограниченного количества элементов множеств $\{O\}$, $\{П\}$, представляющих наиболее характерные закономерности воздействия угроз, функционирования КСИИ и ТР.

Содержание основных закономерностей функционирования КСИИ и ТР определяется их исключительным предназначением, разнообразием используемых технических средств и решаемых задач, обусловливающих свойства и признаки КСИИ, объективностью воздействия угроз и внимания со стороны ТР.

Данные закономерности могут быть представлены соответствующими областями отправления (2) и прибытия (3):

$$O=\{o_1, o_2, \ldots, o_n\}=\{o_i\},\ \ i \in I,\ \ I=1,2, \ldots, n; \tag{2}$$

$$П=\{n_1, n_2, \ldots, n_m\}=\{n_j\},\ \ j \in J,\ \ J=1,2,\ldots, m. \tag{3}$$

Содержательное описание законов соответствия, $C \subset O \times П$, может быть представлено произведением множеств:

$$O\&П=\{(o_i, n_j) |\ o_i \in O;\ \ n_j \in П\};\ \ i = 1, 2, \ldots, n;\ \ j = 1, 2, \ldots, m. \tag{4}$$

Такое множество дает возможность получения ряда соответствий $c = (O, П, C)$, подтверждающих объективность усиленного внимания ТР к КСИИ.

Территориальная распределенность элементов КСИИ, увеличение объемов хранимой и передаваемой информации, жесткие требования к оперативности принятия управленческих решений для своевременного реагирования на нарушения безопасности функционирования объектов приводят к возрастанию количества преднамеренных и непреднамеренных угроз нарушения безопасности информации [5], возможных каналов ее утечки [6] и уязвимых звеньев несанкционированного доступа к информационным ресурсам этих объектов с целью чтения, копирования, подделки программного обеспечения, текстовой и другой информации [7].

С целью выявления возможных угроз, связанных с функционированием КСИИ объектов «критической инфраструктуры», целесообразно использовать базовую модель угроз безопасности информации, разработанную ФСТЭК России.

Нормативную правовую основу системы обеспечения безопасности объектов «критической инфраструктуры» составляют: Конституция Российской Федерации, Стратегия национальной безопасности Российской Федерации до 2020 года, законы Российской Федерации, указы Президента Российской Федерации, постановления Правительства Российской Федерации в сфере безопасности, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, противодействия терроризму и экстремизму, обеспечения правопорядка, борьбы с преступностью.

Основными целями защиты информации в ИКС объектов «критической инфраструктуры» являются:

– достижение состояния защищенности информации во всех звеньях ИКС от внешних и внутренних угроз как в мирное время, так и в особый период, а также при возникновении чрезвычайных ситуаций;

− предотвращение нарушений прав личности, общества и государства на сохранение секретности и конфиденциальности информации, циркулирующей в ИКС.

На основании целей формируются и задачи защиты информации в ИКС объектов «критической инфраструктуры»:

− выявление и прогнозирование внутренних и внешних угроз информационной безопасности, разработка и осуществление комплекса адекватных и экономически обоснованных мер по их предупреждению и нейтрализации;

− формирование единой политики государственной власти и субъектов России по защите информации в ИКС;

− совершенствование и стандартизация применяемых методов и средств защиты информации в ИКС;

− создание и реализация механизма регулирования деятельности в области защиты информации объектов «критической инфраструктуры», а также обеспечение функционирования системы сертификации ИКС и входящих в их состав защищенных технических средств, средств защиты информации и средств контроля эффективности применяемых мер защиты.

Система обеспечения защиты информации в каждой конкретной ИКС, а также подход к ее построению и реализации - индивидуальны. Однако, во всех случаях для создания эффективной комплексной защиты информации необходимо:

1) выявить все возможные факторы, влияющие на уязвимость информации подлежащей защите, т.е. построить модель угроз информационной безопасности ИКС и выявить каналы утечки информации;

2) обосновать возможные методы защиты информации, направленные на устранение выявленных угроз;

3) создать комплексную систему, обеспечивающую качественное решение задач защиты информации в ИКС, основанную на минимизации ущерба от возможной утечки информации.

*Литература*

1. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ № Пр-1895 от 9 сентября 2000 г.

2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Госстандарт России, 2008. – 9 с.

3. Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия–Телеком, 2006. – 544 с.

4. Советов Б.Я. Моделирование систем: учебник для вузов / Б.Я. Советов, С.А. Яковлев. – 3-е изд. – М.: Высш. шк., 2001. – 343 с.

5. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. – Воронеж: Изд-во Воронежского гос. ун-та, 2002. – 408 с.

6. Заряев А.В. Источники и каналы утечки информации в телекоммуникационных системах: учеб. пособие для системы высшего профессионального образования МВД России / А.В. Заряев, В.Б. Щербаков и др. – Воронеж: Воронежский институт МВД России, 2003. – 94 с.

7. Защита информации в телекоммуникационных системах: учебник для вузов МВД России / С.В. Скрыль и др. – Воронеж: Воронежский институт МВД России, 2002. – 300 с.

---

**Авсентьев Олег Сергеевич**
Д-р техн. наук, профессор каф. информационной безопасности
Воронежского института МВД России (ВИ МВД России)
Тел.: (473) 200-52-40
Эл. почта: osaos@mail.ru

**Бабкин Александр Николаевич**
Канд. техн. наук, доцент, нач. каф. информационной безопасности ВИ МВД России
Тел.: (473) 200-52-40
Эл. почта: alex_babk@mail.ru., babkian@mail.vimvd.ru

**Бабкин Сергей Александрович**
Канд. техн. наук, доцент каф. физики
Воронежского института государственной противопожарной службы МЧС России
Тел.: (473) 277-86-53

Avsentjev O.S., Babkin A.N., Babkin S, A.

**Organizational and technical and legal support of safety infocommunication systems of objects «critical infrastructure» in the Russian Federation**

Questions of ensuring information security of objects of «critical infrastructure» in the Russian Federation are considered. Objects of power supply, heat supply, communication and telecommunications, transport infrastructure, law-enforcement system belong to similar objects, etc. The generalized model of key system of information infrastructure is presented.
**Keywords:** information security, object of critical infrastructure, information security, automated control system, infocommunication system.