Документационное обеспечение
систем безопасности объектов КИИ

Владимир АКИМЕНКО,
Центр кибербезопасности критических инфраструктур, АО «ЭЛВИС-ПЛЮС»

Федеральный закон от 26.07.2017 № 187-ФЗ и принятые в соответствии с ним нормативные правовые акты возлагают обязанность создания и обеспечения функционирования систем безопасности объектов критической информационной инфраструктуры (далее – объектов КИИ) на государственные органы, государственные учреждения, российские юридические лица, индивидуальных предпринимателей, владеющих на законном основании объектами КИИ (далее – субъекты КИИ).

Требования к документационному обеспечению

Указанные выше нормативные правовые акты и методические документы не содержат конкретных рекомендаций по общему составу, структуре и содержанию документов, регламентирующих создание, организацию эксплуатации и обеспечение функционирования систем/подсистем безопасности объектов КИИ.

Как правило, в организациях уже внедрена система внутренней нормативной документации, регламентирующая управленческие процессы, в том числе определяющая требования к составу, структуре и содержанию документов, связанных с обеспечением информационной безопасности в организации. Однако, если такие требования не установлены, каждый субъект КИИ вынужден самостоятельно определять состав, структуру и содержание требуемых документов.

В настоящей статье на основе анализа существующих стандартов, отечественных и международных практик, требований нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры, а также опыта выполнения работ в интересах различных организаций рассмотрен возможный состав, структура и общее содержание документационного обеспечения процессов создания, организации эксплуатации и обеспечения функционирования систем/подсистем безопасности значимых объектов КИИ.

Структура документационного обеспечения

С точки зрения назначения, области применения, а также общих стадий и этапов создания, процессов организации эксплуатации и обеспечения функционирования систем/подсистем безопасности документационное обеспечение в части обеспечения безопасности значимых объектов КИИ может быть структурировано по следующим группам документов.

1. Общекорпоративные документы, определяющие высокоуровневые цели, задачи, направления деятельности и обязанности руководства по обеспечению безопасности объектов КИИ и безопасности информации в организации в целом (стратегии, концепции, политики).
2. Документы, определяющие требования и описывающие систему безопасности значимых объектов КИИ, включая требования и положения по структуре и функционированию системы безопасности (стандарты организации, положения, требования, частные политики).
3. Документы, определяющие организационную структуру систем безопасности значимых объектов КИИ, в том числе описание функций, задач и зон ответственности подразделений и/или отдельных работников по организации или обеспечению безопасности объектов КИИ (приказы/распоряжения, положения о подразделении, должностные инструкции).
4. Документы на подсистему безопасности значимых объектов КИИ, определяющие требования к созданию, описывающие принципы, механизмы, способы и средства, обеспечивающие развертывание, функционирование и эксплуатацию подсистем безопасности значимых

объектов КИИ (технические требования, задания, модели, проектная и эксплуатационная документация).

5. Документы, определяющие способы, правила и порядок (процедуры) реализации мероприятий по обеспечению безопасности значимых объектов КИИ в рамках установленных процессов деятельности (регламенты, руководства, инструкции, методические рекомендации).
6. Документы, отражающие состояние безопасности и определяющие планы по управлению деятельностью по обеспечению безопасности значимых объектов КИИ (планы, отчеты, журналы учета).

Указанные группы документов должны быть увязаны в соответствии с установленной иерархией документов, определяемой субъектом КИИ.

Состав разрабатываемых документов

При определении документационного обеспечения процессов создания, организации эксплуатации и обеспечения функционирования систем/подсистем безопасности объектов КИИ перед субъектами КИИ определяющими становятся два вопроса: какой состав конкретных документов выбрать и каково должно быть их содержание?

Требованиями подзаконных нормативных актов по обеспечению безопасности значимых объектов КИИ, выпущенных ФСТЭК России и ФСБ России, определены лишь некоторые требования к составу и содержанию указанных документов.

С учетом требований названных подзаконных нормативных правовых актов минимальный и для большинства случаев достаточный состав разрабатываемых документов по обеспечению безопасности значимых объектов КИИ может выглядеть следующим образом.

Наименование (содержание) документа	Основание для разработки
Документы первой группы	
Концепция (политика) обеспечения безопасности значимых объектов КИИ – документ, предназначенный для определения позиции организации по вопросам обеспечения безопасности информации и безопасности объектов КИИ, включающий описание: • целей и задач обеспечения безопасности; • объектов защиты (информации, архитектуры, средств, конфигураций); • основных угроз безопасности информации и категорий нарушителей; • рисков и возможных негативных последствий; • подходов к способам, механизмам обеспечения безопасности информации и объектов КИИ, выбору средств защиты информации (далее – СЗИ); • ответственность за соблюдение и нарушение требований и правил обеспечения безопасности	п. 25-а требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235
Документы второй группы	
Стандарт (требования) по обеспечению безопасности значимых объектов КИИ, включающий описание: • требований и правил обеспечения, управления, контроля, анализа состояния и оценки соответствия требованиям по безопасности значимых объектов КИИ; • состава основных организационных и технических мер по обеспечению безопасности значимых объектов КИИ на этапах жизненного цикла; • требований к уровню подготовки и проверки знаний и умений работников, участвующих в обеспечении безопасности значимых объектов КИИ	п. 23, 25-а, 33, 34 требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 п. 12.2, 13.1-в, 13.6, 13.7, 14 требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239
Положение о системе безопасности значимых объектов КИИ, включающее описание состава, структуры, задач (функций), функционирования и взаимодействия компонентов системы безопасности и ее участников, а также описание применяемых мер по обеспечению безопасности значимых объектов КИИ, включая: • организацию разработки, утверждения и внесения изменений в План мероприятий по обеспечению безопасности значимых объектов КИИ, а также контроля его исполнения и документирования результатов; • организацию реализации (внедрения) мероприятий по обеспечению безопасности значимых объектов КИИ; • управление (администрирование), обеспечение эксплуатации и контроль функционирования СЗИ; • управление и контроль изменений конфигураций; • контроль физического доступа к объектам КИИ; • анализ угроз и уязвимостей (включая определение периодичности проведения анализа); • мониторинг и контроль состояния безопасности значимых объектов КИИ, включая описание правил выявления компьютерных атак и компьютерных инцидентов; • обеспечение безопасности объектов КИИ при возникновении нештатных ситуаций; • совершенствование безопасности значимых объектов КИИ; • информирование, обучение, тренировки и контроль осведомленности персонала; • сопровождение функционирования системы безопасности, ведения документации; • проведение испытаний, приемки и оценки соответствия СЗИ требованиям по безопасности	п. 8, п. 9, п. 22, п. 25-а, 25-б, раздел V требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 п. 12.3, п. 13.1б-в, п. 13.2, п. 13.3б-ж, п. 13.4б-г требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239

Наименование (содержание) документа	Основание для разработки
Документы третьей группы	
Положение о постоянно действующей комиссии по категорированию объектов КИИ, включая описание целей и основных задач деятельности комиссии, ее состава и структуры, режима (плана) работы, прав и зон ответственности, уровня подчиненности, вопросов взаимодействия с другими подразделениями субъекта КИИ и внешними организациями	п. 11 правил, утвержденных Постановлением Правительства РФ от 08.02.2018 № 127 *Вводится в действие приказом/распоряжением
Положение о структурном подразделении, ответственном за обеспечение безопасности объектов КИИ (или приказ/распоряжение о назначении отдельных работников, ответственных за обеспечение безопасности значимых объектов КИИ), включая описание целей и основных задач, состава и структуры подразделения, прав и зон ответственности, уровня подчиненности, взаимодействия с другими подразделениями субъекта КИИ и внешними организациями	п. 10 требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 *Вводится в действие приказом/распоряжением
Приказ (распоряжение) о назначении работников, ответственных за планирование и контроль мероприятий по обеспечению безопасности значимых объектов КИИ	п. 13.1-а требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239
Приказ (распоряжение) о назначении работников, ответственных за управление (администрирование) подсистемой безопасности значимых объектов КИИ (администраторов безопасности), а также ответственных за внесение изменений в конфигурацию значимых объектов КИИ и их подсистем безопасности	п. 12.3-г, п. 13.3-а, п. 13.4-а требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235
Приказ (распоряжение) об определении работника, ответственного за выявление компьютерных инцидентов и реагирование на них, с определением зон ответственности, функций (задач), включая задачи по организации тренировок отработки мероприятий по реагированию и восстановлению	п. 13.5 требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239 п. 10 порядка, утвержденного приказом ФСБ России от 19.06.2019 № 282
Положение о комиссии по контролю состояния безопасности значимых объектов КИИ, включая описание состава и структуры комиссии, порядка и периодичности проведения контроля, критериев оценки эффективности организации работ по обеспечению безопасности значимых объектов КИИ, требований к документированию результатов осуществления внутреннего контроля	п. 35, п. 36 требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 *Комиссия может не создаваться, если субъектом КИИ принято решение о проведении внешней оценки (аудита)
Должностная инструкция работника, ответственного за обеспечение безопасности значимых объектов КИИ, включая описание функциональных обязанностей (в том числе задач по анализу угроз, реагированию на компьютерные инциденты, проведению оценки соответствия), прав, зон ответственности, подчиненности, требований к уровню знаний и умений	п. 10, п. 12, п. 13 требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235
Должностные инструкции работников, ответственных за эксплуатацию и обеспечение функционирования значимых объектов КИИ (дополнения в них), в части описания функциональных обязанностей (задач) и ответственности по обеспечению безопасности значимых объектов КИИ	п. 14 требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235
Документы четвертой группы	
Техническое задание на создание подсистемы безопасности значимых объектов КИИ, включая указание целей и задач обеспечения безопасности, категории значимости, перечень типов объектов защиты, описание требований к составу мер, структуре, функциям, видам обеспечения, средствам, составу и содержанию разрабатываемой документации, а также порядку создания, проведения испытаний, приемки и вводу подсистемы в действие	п. 10 требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239
Модель угроз и нарушителя безопасности информации значимых объектов КИИ, включая краткое описание объектов КИИ, источников угроз, уязвимостей, возможных способов реализации угроз, возможных последствий от реализации (возникновения) угроз *Документ разрабатывается в соответствии с методическими документами ФСТЭК России	п. 25-б требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 п. 11, п. 11.1 требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239
Комплект проектной документации на подсистему безопасности значимых объектов, в составе документов: • Ведомость проектных документов; • Пояснительная записка (описывающая функциональную и техническую архитектуру, субъекты, объекты и политики доступа, состав реализуемых мер, виды и типы применяемых СЗИ, требования к внешнему взаимодействию, организационную структуру, а также требования к параметрам настройки средств); • Схема структурная системы; • Схема (описание) информационных потоков; • Схема (описание) сегментации (адресации); • План расположения, чертеж установки, схема соединений (при наличии технических средств); • Спецификация; • Программа опытной эксплуатации; • Программа и методика испытаний (включая методику анализа уязвимостей) – документ может включаться в состав комплекта эксплуатационной документации или разрабатываться отдельно; • Сметные расчеты (при необходимости)	п. 11.2, пп.12.4–12.7 требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239 *При внедрении и вводе в действие могут разрабатываться и оформляться и иные документы, обеспечивающие ввод в действие подсистемы безопасности значимых объектов КИИ
Комплект эксплуатационной документации на подсистему безопасности значимых объектов КИИ, определяющей порядок и правила эксплуатации СЗИ, в составе документов: • Ведомость эксплуатационных документов; • Руководство администратора (включая порядок и параметры настроек СЗИ, обеспечивающих безопасность объекта КИИ); • Руководство пользователя (включая правила работы пользователей с СЗИ); • Инструкция по эксплуатации средств (включая правила эксплуатации СЗИ); • Формуляр	п. 13.4-в, п. 11.3, п. 22 требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235

Наименование (содержание) документа	Основание для разработки
Документы пятой группы	
Регламент(ы) реализации отдельных мер по обеспечению безопасности значимых объектов КИИ, включая описание порядка выполнения процедур и взаимодействия подразделений (работников), при организации и реализации следующих мер: • управления и поддержания в актуальном состоянии учетных записей пользователей (субъектов доступа) и правил разграничения доступа; • обеспечения антивирусной защиты; • резервного копирования и восстановления; • управления средствами защиты информации; • управления обновлениями безопасности; • управления изменениями конфигураций; • контроля (анализа) защищенности; • выявления компьютерных атак и компьютерных инцидентов; • анализа и оценки функционирования значимых объектов КИИ, включая анализ и устранение уязвимостей и иных недостатков; • организации информирования, обучения, проверки знаний и правил эксплуатации отдельных СЗИ; • организации планирования, внедрения и отработки действий работников по обеспечению безопасности значимых объектов КИИ при возникновении нештатных ситуаций и принятия мер по недопущению их повторного возникновения; • организации и обеспечения безопасности объекта КИИ при выводе его из эксплуатации; • организации гарантийного и (или) технического обслуживания и сопровождения	п. 25-б требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 п. 12.2, п. 13.3-б–13.3-д), 13.4-б–13.4-г, 13.6, 13.7, 13.8, 14 требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239
Регламент (план) реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, включая определение: • состава значимых объектов КИИ и их характеристик; • состава подразделений и лиц, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак, их задач и зон ответственности; • условия (события) начала и порядка реагирования на компьютерные инциденты, включая регламентное время реагирования; • порядка восстановления функционирования значимых объектов КИИ, включая регламентное время восстановления; • объем, содержание и периодичность проведения тренировок по отработке мероприятий	п. 25-б требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 п. 13.5, 13.6-д требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239 п. 6 порядка, утвержденного приказом ФСБ России от 19.06.2019 № 282
Регламент взаимодействия с ГосСОПКА, включая определение: • порядка информирования о компьютерных инцидентах; • порядка обмена информацией о компьютерных инцидентах; • порядка информирования о результатах мероприятий по реагированию на компьютерные инциденты	п. 25-б) требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 п. 2 – п. 5 требований, утвержденных приказом ФСБ России от 19.06.2019 № 282 приказ ФСБ России от 24.07.2018 № 368
Инструкция по безопасной работе работников на значимых объектах КИИ, включая описание действий работников при возникновении компьютерных инцидентов и иных нештатных ситуаций	п. 25-в требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 п. 12.2 требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239
Документы шестой группы	
План мероприятий по обеспечению безопасности значимых объектов КИИ, включая перечень мероприятий, обоснование необходимости их проведения, сроки, ответственных за их проведение и контроль выполнения, в том числе мероприятий по защите информации, недопущения несанкционированного воздействия на нее, проверке механизмов восстановления работоспособности значимого объекта КИИ, совершенствованию процессов обеспечения безопасности объектов КИИ, организации обучения и проверки знаний работников, непрерывному взаимодействию с ГосСОПКА	п. 25-б, п. 29, п. 30 требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 п.13.1-б – п. 13.1-в требований, утвержденных приказом ФСТЭК России от 25.12.2017 № 239
Комплект документов по результатам работы комиссии по категорированию, включая: • Перечень объектов КИИ, подлежащих категорированию; • Акт категорирования объектов КИИ с приложением (при необходимости) обоснования присвоения категорий значимости; • Сведения о категорировании объектов КИИ	п. 15 – п. 17 правил, утвержденных Постановлением Правительства РФ от 08.02.2018 № 127
Акт работы комиссии по контролю состояния безопасности объектов КИИ, в который включаются итоги проверки комиссией результатов внутреннего контроля организации работ по обеспечению безопасности значимых объектов КИИ	п. 36 требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235 *Акт оформляется в случае создания Комиссии
Отчет о выполнении Плана мероприятий по обеспечению безопасности значимых объектов КИИ, включая сведения о результатах выполнения мероприятий по обеспечению безопасности, а также предложения по развитию системы безопасности и совершенствованию мер обеспечения безопасности значимых объектов КИИ	п. 32, п. 37 требований, утвержденных приказом ФСТЭК России от 21.12.2017 № 235

Не догма, но пример

Разумеется, представленный выше комплект документов не является догмой и должен рассматриваться каждым конкретным субъектом КИИ в качестве примера, а содержание указанных документов должно определяться как с точки зрения структуры, особенностей деятельности организации, состава и характеристик объектов КИИ, так и с учетом сложившейся в организации практики документооборота, существующих требований и действующих в организации локальных нормативных документов в области обеспечения информационной безопасности.■

elvis.ru