Беркин Матвей Алексеевич,
студент, РТУ МИРЭА

РАЗРАБОТКА ТИПОВЫХ РЕГЛАМЕНТОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. В статье рассмотрены вопросы разработки организационно-распорядительной документации, предназначенной для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее – КИИ). Проведен анализ нормативно-правовой базы в области обеспечения безопасности объектов КИИ, рассмотрены особенности категорирования объектов критической информационной инфраструктуры и влияние категории значимости на состав реализуемых мер защиты информации.

Ключевые слова: Критическая информационная инфраструктура, защита информации, информационная безопасность, регламент, организационно-распорядительная документация, меры защиты информации.

Введение

Цифровая трансформация государственных органов, промышленных предприятий и организаций различных отраслей экономики привела к существенному увеличению количества информационных систем, обеспечивающих выполнение критически важных процессов. Нарушение функционирования таких систем может привести к возникновению значительных экономических потерь, нарушению производственных процессов, снижению качества предоставляемых услуг и созданию угроз безопасности государства.

Для обеспечения устойчивого функционирования информационной инфраструктуры в Российской Федерации сформирована система нормативного регулирования в области безопасности критической информационной инфраструктуры. Одним из ключевых направлений данной деятельности является обеспечение безопасности значимых объектов КИИ посредством реализации комплекса организационных и технических мер защиты информации.

Практика обеспечения информационной безопасности показывает, что применение технических средств защиты не может обеспечить необходимый уровень защищенности без установления единых правил эксплуатации информационных систем и закрепления обязанностей участников процессов защиты информации. В связи с этим особое значение приобретают организационно-распорядительные документы, определяющие порядок выполнения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Основная часть

Нормативно-правовые основы обеспечения безопасности объектов КИИ

Правовые основы обеспечения безопасности объектов критической информационной инфраструктуры определяются Федеральным законом от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Указанный нормативный акт устанавливает требования к субъектам КИИ, определяет порядок категорирования объектов и закрепляет обязанности по обеспечению их безопасности.

Общие требования к защите информации определяются Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Данный закон устанавливает основные принципы защиты информации и определяет необходимость предотвращения неправомерного доступа к информационным ресурсам.

Стратегические направления развития системы информационной безопасности определяются Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации № 646. Дополнительные требования по организации защиты информации содержатся в Указе Президента Российской Федерации № 250, направленном на повышение уровня защищенности информационной инфраструктуры организаций.

Порядок категорирования объектов критической информационной инфраструктуры установлен Постановлением Правительства Российской Федерации № 127. Документ определяет критерии значимости объектов и порядок присвоения категорий значимости в зависимости от возможных последствий нарушения их функционирования.

Важное значение имеет Распоряжение Правительства Российской Федерации № 360-р, содержащее перечень типовых отраслевых объектов критической информационной инфраструктуры Российской Федерации. Использование данного перечня позволяет определить принадлежность конкретных информационных систем к объектам КИИ соответствующей отрасли.

Непосредственные требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования установлены приказами ФСТЭК России № 235 и № 239. Эти документы являются основой практической реализации мероприятий по защите информации на значимых объектах критической информационной инфраструктуры.

Влияние категории значимости на организацию защиты информации

Одним из основных этапов обеспечения безопасности объектов критической информационной инфраструктуры является проведение категорирования. В ходе данной процедуры осуществляется анализ возможных последствий нарушения функционирования объекта, а также определяется его значимость для государства, экономики и общества.

По результатам категорирования объекту присваивается первая, вторая или третья категория значимости. Категория значимости определяет объем требований, предъявляемых к системе безопасности объекта, перечень обязательных мер защиты информации и уровень контроля за их реализацией.

Чем выше категория значимости объекта КИИ, тем более широкий перечень мер безопасности должен быть реализован субъектом критической информационной инфраструктуры. Одновременно возрастают требования к процессам мониторинга событий безопасности, регистрации инцидентов, контролю состояния информационной инфраструктуры и документированию мероприятий по защите информации.

Категория значимости оказывает влияние не только на выбор технических средств защиты, но и на состав организационно-распорядительной документации. Для каждого значимого объекта КИИ должны быть определены внутренние процедуры эксплуатации, администрирования, контроля и реагирования на события безопасности, обеспечивающие выполнение требований нормативных документов.

Таким образом, разработка регламентов напрямую связана с результатами категорирования объекта КИИ и должна учитывать установленную категорию значимости, архитектуру информационной инфраструктуры, состав обрабатываемой информации и актуальные угрозы безопасности.

Роль регламентов в системе обеспечения безопасности объектов КИИ

Организационно-распорядительная документация является неотъемлемой частью системы обеспечения безопасности значимых объектов критической информационной инфраструктуры. Основная задача таких документов заключается в формализации процессов защиты информации и установлении единых требований к действиям работников организации.

Регламенты определяют порядок выполнения мероприятий по защите информации, распределяют ответственность между участниками процессов обеспечения безопасности и

устанавливают механизмы контроля выполнения требований безопасности. Наличие регламентов позволяет исключить неоднозначность при выполнении работ, связанных с эксплуатацией информационных систем и средств защиты информации.

Разработка регламентов осуществляется на основании требований законодательства Российской Федерации, нормативных документов ФСТЭК России, результатов категорирования объекта КИИ, модели угроз безопасности информации и особенностей функционирования информационной инфраструктуры.

Содержание регламентов определяется реализуемыми мерами защиты информации и должно учитывать специфику конкретного объекта критической информационной инфраструктуры. При изменении архитектуры информационной системы, появлении новых угроз безопасности информации или изменении нормативных требований регламенты подлежат актуализации.

Регламентация мер защиты информации

В соответствии с приказом ФСТЭК России № 239 обеспечение безопасности значимых объектов критической информационной инфраструктуры осуществляется посредством реализации комплекса организационных и технических мер защиты информации. Перечень реализуемых мер определяется категорией значимости объекта КИИ, особенностями его функционирования, составом информационной инфраструктуры и актуальными угрозами безопасности информации.

Одной из базовых мер является идентификация и аутентификация субъектов и объектов доступа. Реализация данной меры обеспечивает подтверждение подлинности пользователей и устройств, получающих доступ к информационным ресурсам. Для ее выполнения устанавливаются процедуры создания, изменения, блокирования и удаления учетных записей, а также правила использования средств аутентификации.

Важное значение имеет управление доступом к информационным ресурсам. Данная мера обеспечивает разграничение прав пользователей и исключает возможность выполнения действий, не предусмотренных их должностными обязанностями. Регламентация управления доступом определяет порядок предоставления прав доступа, их пересмотра и контроля использования.

Одним из ключевых элементов обеспечения безопасности является регистрация событий безопасности. Средства регистрации обеспечивают фиксацию действий пользователей, администраторов и программных компонентов информационной системы. Журналы событий используются для выявления нарушений безопасности, расследования инцидентов и контроля соблюдения требований нормативных документов.

Для противодействия вредоносному программному обеспечению реализуются меры антивирусной защиты. Они предусматривают использование специализированных программных средств, обновление сигнатурных баз и проведение периодических проверок информационных ресурсов. Данные мероприятия позволяют снизить вероятность заражения информационной инфраструктуры вредоносным программным обеспечением.

Существенную роль в обеспечении безопасности играет управление обновлениями программного обеспечения. Большинство современных компьютерных атак связано с эксплуатацией известных уязвимостей программных продуктов. В связи с этим должны быть установлены процедуры поиска обновлений, проверки их подлинности, тестирования, установки и контроля результатов внедрения обновлений.

Неотъемлемой частью системы безопасности является защита машинных носителей информации. Для съемных и стационарных носителей информации устанавливаются правила учета, хранения, выдачи, использования, транспортировки и уничтожения. Контроль обращения с носителями позволяет снизить риск утечки информации и предотвратить несанкционированный перенос данных.

Особое место занимает защита технических средств и систем. Данная мера направлена на предотвращение несанкционированного физического воздействия на оборудование,

используемое для обработки информации. Для ее реализации организуются контролируемые зоны, ограничивается физический доступ к оборудованию, обеспечивается защита от внешних воздействий и устанавливаются правила эксплуатации технических средств.

Для своевременного выявления нарушений безопасности применяются средства обнаружения вторжений и мониторинга событий безопасности. Их использование позволяет выявлять признаки компьютерных атак на ранних этапах и принимать меры по предотвращению развития инцидентов.

Важной составляющей системы защиты является контроль целостности информации и программного обеспечения. Реализация данной меры позволяет выявлять несанкционированные изменения данных, программных компонентов и конфигураций информационных систем.

Для обеспечения устойчивого функционирования значимых объектов КИИ реализуются меры обеспечения доступности информации. К ним относятся резервирование критически важных компонентов инфраструктуры, резервное копирование данных и мероприятия по восстановлению работоспособности после возникновения отказов и сбоев.

При использовании технологий виртуализации дополнительно реализуются меры защиты среды виртуализации. Их целью является предотвращение несанкционированного взаимодействия между виртуальными машинами и обеспечение безопасности виртуальной инфраструктуры.

Отдельную группу мероприятий составляет управление конфигурацией. Данная мера предусматривает контроль изменений аппаратного и программного обеспечения, учет конфигурационных единиц и документирование выполняемых изменений. Реализация управления конфигурацией позволяет поддерживать актуальное состояние информационной инфраструктуры и снижает вероятность возникновения ошибок эксплуатации.

Не менее важным элементом обеспечения безопасности является реагирование на компьютерные инциденты. Для этих целей определяются процедуры выявления, регистрации, анализа и устранения последствий инцидентов информационной безопасности. Наличие регламентированного порядка реагирования позволяет минимизировать последствия компьютерных атак и сократить время восстановления работоспособности информационных систем.

Практическая реализация перечисленных мер невозможна без разработки организационно-распорядительной документации. Регламенты закрепляют обязанности должностных лиц, устанавливают порядок выполнения мероприятий по защите информации и определяют механизмы контроля их исполнения. Содержание таких документов зависит от категории значимости объекта КИИ, состава информационной инфраструктуры, модели угроз безопасности информации и требований действующего законодательства.

Заключение

Обеспечение безопасности значимых объектов критической информационной инфраструктуры представляет собой комплексную задачу, включающую реализацию взаимосвязанных организационных и технических мер защиты информации. Анализ нормативно-правовой базы показал, что основой данной деятельности являются требования Федерального закона № 187-ФЗ, Постановления Правительства Российской Федерации № 127 и приказов ФСТЭК России № 235 и № 239.

Установлено, что состав мер защиты информации определяется категорией значимости объекта КИИ и зависит от особенностей функционирования информационной инфраструктуры, состава обрабатываемой информации и актуальных угроз безопасности. Реализация требований безопасности требует не только применения технических средств защиты, но и разработки комплекса организационно-распорядительных документов.

Проведенный анализ показал, что регламенты являются одним из основных инструментов практической реализации требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Они обеспечивают единообразное

выполнение процедур безопасности, распределение ответственности между участниками процессов защиты информации и контроль соблюдения требований нормативных документов.

Таким образом, разработка и актуализация регламентов позволяет повысить уровень защищенности объектов критической информационной инфраструктуры, обеспечить выполнение обязательных требований законодательства Российской Федерации и создать условия для устойчивого функционирования информационных систем в условиях современных угроз информационной безопасности

Список литературы:

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

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

3. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации…».

4. Распоряжение Правительства Российской Федерации № 360-р «Об утверждении перечня типовых отраслевых объектов критической информационной инфраструктуры Российской Федерации».

5. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

6. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

7. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

8. ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности.

9. Ерохин С. Д., Петухов А. Н., Пилюгин П. Л. Управление безопасностью критических информационных инфраструктур. М.: Горячая линия – Телеком, 2021. 240 с.

10. Казарин О. В., Шубинский И. Б. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие. М.: Юрайт, 2024. 342 с