

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
ПО РАЗРАБОТКЕ ПЛАНА РЕАГИРОВАНИЯ НА
КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ И ПРИНЯТИЯ МЕР ПО
ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК,
ПРОВЕДЕННЫХ В ОТНОШЕНИИ ЗНАЧИМЫХ ОБЪЕКТОВ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Оглавление

1. Перечень сокращений.....	4
2. Общие положения.....	6
3. Нормативные ссылки	8
4. Требования к разработке Плана.....	12
5. Разделы Плана	15
5.1. Раздел 1. Технические характеристики и состав ЗОКИИ.	15
5.2. Раздел 2. События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий.	15
5.3. Раздел 3. Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию.....	17
5.4. Раздел 4. Описание состава подразделений и должностных лиц субъекта КИИ, ответственных за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА.....	19
5.5. Раздел 5. Условия привлечения подразделений и должностных лиц ФСБ России <i>(при необходимости)</i>	20
5.6. Раздел 6. Порядок проведения мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА в отношении ЗОКИИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России <i>(при необходимости)</i>	21
6. Очередность реагирования на КИ	24
6.1. Определение уровня влияния КИ.	25
6.2. Определение приоритетов КИ и очередности реагирования на КИ.	27
7. Организация взаимодействия	30
7.1. Взаимодействие с подразделениями внутри организации.	31
7.2. Взаимодействие субъекта КИИ с курирующим ОИВ.	31
7.3. Взаимодействие с поставщиками услуг (подрядчиками).....	31
7.4. Взаимодействие с ФСБ России.	31
7.4.1. Взаимодействие при КИ в период проведения ФСБ России оценки защищенности.....	32
7.5. Взаимодействие в ГосСОПКА и НКЦКИ.....	35
7.6. Взаимодействия с Роскомнадзором.	37
7.7. Взаимодействие со ФСТЭК России.....	40
7.8. Взаимодействие с другими субъектами КИИ.	40
7.9. Взаимодействие с лицензиатами и внешними центрами поддержки.	40
7.10. Взаимодействие с внешними и отраслевыми регуляторами.....	40
7.11. Взаимодействие с правоохранительными органами.....	41
7.12. Взаимодействие со СМИ.....	41
8. Средства реагирования	42

9. Обеспечение процессов реагирования.....	44
10. Маркеры (вехи) при выполнении этапов Плана.....	45
11. Порядок действий, разработанный ФСТЭК России, по обеспечению безопасности объектов КИИ и технической защиты информации в органах государственной власти и организациях при реализации угроз безопасности информации	46
12. Заключение	47
Приложение 1.....	48
Приложение 2.....	49
Приложение 3.....	50
Приложение 4.....	76
Приложение 5	78
Приложение 6.....	79
Приложение 7.....	80
Приложение 8.....	81
Приложение 9.....	86
Приложение 10.....	88
Приложение 11.....	89
Приложение 12.....	90
Приложение 13.....	91

1. Перечень сокращений

В настоящем документе используются сокращения, приведенные в таблице 1.

Таблица 1. Перечень сокращений

Сокращение	Обозначение
АСУ ТП	Автоматизированная система управления технологическим процессом
ВПО	Вредоносное программное обеспечение
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ДИТ	Департамент информационных технологий города Москвы
ЗОКИИ	Значимый объект критической информационной инфраструктуры Российской Федерации
ИБ	Информационная безопасность
КА	Компьютерная атака
КИ	Компьютерный инцидент
КИИ	Критическая информационная инфраструктура Российской Федерации
КоАП РФ	Кодекс Российской Федерации об административных правонарушениях
Личный кабинет субъекта ГосСОПКА	Личный кабинет субъекта ГосСОПКА, зарегистрированный в технической инфраструктуре НКЦКИ, предназначенный для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными
Минпромторг России	Министерство промышленности и торговли Российской Федерации
Минцифры России	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Минтранс России	Министерство транспорта Российской Федерации
Минэнерго России	Министерство энергетики Российской Федерации
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
ОКИИ	Иные объекты критической информационной инфраструктуры Российской Федерации, не отнесенные к одной из категорий значимости
ОИВ	Орган исполнительной власти города Москвы
Орган (организация)	Органы исполнительной власти города Москвы, подведомственные им государственные учреждения города Москвы, находящиеся в их ведомственном подчинении государственных унитарных предприятий города Москвы

ПАК	Программно-аппаратный комплекс
ПДн	Персональные данные
План	План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на значимые объекты критической информационной инфраструктуры Российской Федерации
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
РФ	Российская Федерация
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
СМИ	Средство массовой информации
Структурное подразделение	Структурное подразделение органа (организации)
ФОИВ	Федеральный орган исполнительной власти
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ЦОД	Центр обработки данных
ЦОДД	Центр организации дорожного движения

2. Общие положения

Настоящие Методические рекомендации разработаны в целях методического обеспечения деятельности субъектов КИИ, которым на праве собственности, аренды или ином законном основании принадлежат ЗОКИИ.

Методические рекомендации предназначены для использования субъектами КИИ при разработке Плана реагирования на КИ и принятия мер по ликвидации последствий КА (далее – План).

Методические рекомендации содержат общую схему взаимодействия субъектов КИИ с органами государственной власти города Москвы и иными организациями при реагировании на КИ и принятия мер по ликвидации последствий компьютерных атак.

Основные понятия, которые употребляются в настоящих Методических рекомендациях определены Федеральными законами от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и от 27.07.2006 № 152-ФЗ «О персональных данных» за исключением случаев, указанных особо, а также ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» утвержденным приказом Росстандарта от 29 ноября 2022 года № 1375-ст.

Мероприятия, проводимые в ходе реагирования на КИ и принятия мер по ликвидации последствий КА в отношении ЗОКИИ, приведены на рисунке 1.

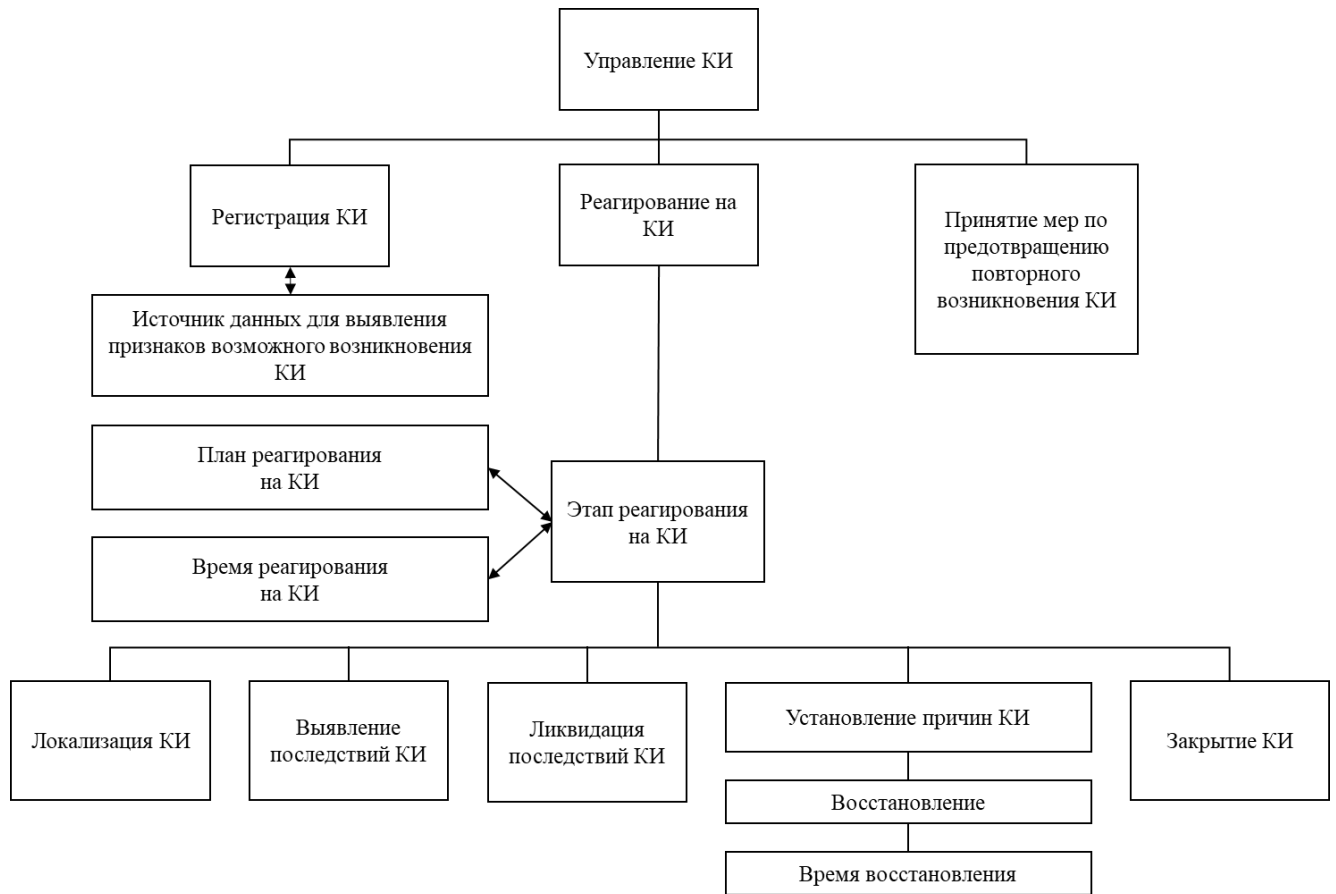


Рис. 1. Мероприятия, проводимые в ходе реагирования на КИ и принятия мер по ликвидации последствий КА

3. Нормативные ссылки

Настоящие Методические рекомендации разработаны с учетом требований законодательства Российской Федерации:

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ;

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

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

4. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

5. Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

6. Постановление Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»;

7. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

8. Приказ ФСБ России от 13.02.2023 № 77 «Об утверждении Порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных»;

9. Приказ ФСБ России от 11.05.2023 № 213 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам,

являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими»;

10. Приказ ФСБ России от 23.12.2025 № 539 «Об утверждении Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

11. Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам»;

12. Приказ ФСБ России от 25.12.2025 № 546 «Об утверждении Порядка обмена информацией о компьютерных атаках и компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты»;

13. Приказ ФСБ России от 25.12.2025 № 547 «Об утверждении Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

14. Приказ ФСБ России от 25.12.2025 № 548 «Об утверждении Порядка осуществления непрерывного взаимодействия субъектов критической информационной инфраструктуры Российской Федерации, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры Российской Федерации, а также руководителей органов и организаций, на которых возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

15. Приказ ФСБ России от 26.12.2025 № 553 «Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе средств, предназначенных для поиска признаков компьютерных атак, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»;

16. Приказ ФСБ России от 26.12.2025 № 554 «Об установлении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе к средствам, предназначенным для поиска признаков компьютерных атак»;

17. Приказ Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных»;

18. 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»;

19. Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

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

21. Постановление Правительства Москвы от 23.12.2021 № 2170-ПП «Об утверждении Положения о координации деятельности органов исполнительной власти города Москвы и подведомственных им организаций в области обеспечения безопасности информации, обрабатываемой с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях»;

22. Распоряжение Департамента информационных технологий города Москвы от 12.09.2022 № 64-16-434/22 «Об утверждении порядка предоставления сведений об инцидентах информационной безопасности»;

23. Рекомендации ФСТЭК России по повышению уровня безопасности информационных ресурсов при установлении в Российской Федерации уровней опасности проведения целевых компьютерных атак;

24. Методический документ «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (утв. ФСТЭК России 11.11.2025);

25. Методические рекомендации по организации прямого взаимодействия с НКЦКИ (утв. НКЦКИ 02.09.2024);

26. Методические рекомендации НКЦКИ по разработке Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации;

27. Методические рекомендации НКЦКИ по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации;

28. Инструкция НКЦКИ по формированию электронного письма уведомления о компьютерном инциденте, атаке или уязвимости;

29. Регламент взаимодействия Национального координационного центра по компьютерным инцидентам и владельцев информационных ресурсов Российской Федерации при информировании Федеральной службы безопасности Российской Федерации о компьютерных инцидентах, реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак (утв. НКЦКИ 02.09.2024);

30. ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» утвержден приказом Росстандарта от 29 ноября 2022 года № 1375-ст;

31. ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения» утвержден приказом Росстандарта от 29 ноября 2022 года № 1376-ст;

32. ГОСТ Р 59711-2022 «Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами» утвержден приказом Росстандарта от 29 ноября 2022 года № 1377-ст;

33. ГОСТ Р 59712-2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты» утвержден приказом Росстандарта от 29 ноября 2022 года № 1378-ст.

4. Требования к разработке Плана

При разработке Плана учитывать организационную структуру субъекта КИИ, назначение и архитектуру ЗОКИИ, применяемые программные и программно-аппаратные средства, взаимосвязь с другими объектами КИИ, наличие и характеристики доступа к сетям связи [26¹].

План включает следующие разделы:

1. Технические характеристики и состав ЗОКИИ;
2. События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий;
3. Мероприятия, проводимые в ходе реагирования на КИ и принятия мер по ликвидации последствий КА, а также время, отводимое на их реализацию;
4. Описание состава подразделений и должностных лиц субъекта КИИ, ответственных за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА.

План может содержать дополнительные разделы:

5. Условия привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА.
6. Порядок проведения мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА в отношении ЗОКИИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России.

Силы ФСБ России включаются в План при объективной оценке неготовности подразделений ИБ субъекта КИИ к проведению в полном объеме мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА.

Проект Плана, содержащий положения, предусмотренные пунктом 7 Порядка информирования ФСБ России о КИ, реагирования на них, принятия мер по ликвидации последствий КА, проведенных в отношении ЗОКИИ [13], разрабатываются субъектом КИИ и до его утверждения направляется на согласование в ФСБ России.

Рекомендуемая форма сопроводительного письма о направлении на согласование Плана в ФСБ России приведена в приложении 1 к настоящим Методическим рекомендациям.

7. Разделы или положения, касающиеся порядка пересмотра Плана.
8. Разделы или положения, содержащие информацию или реквизиты, которые являются обязательными при составлении локальных нормативных актов в соответствии с правилами ведения делопроизводства субъекта КИИ.

План может также включать в себя различные приложения, например инструкции, регламенты и иные документы, в соответствии с которыми осуществляется деятельность по обнаружению, регистрации, принятию решений и действий, связанных с реагированием на КИ в городе Москве [13], [21].

¹ Здесь и далее в настоящих Методических рекомендациях указывается отсылка к порядковому номеру в разделе Нормативные ссылки.

При разработке Плана должны учитываться положения документов, разработанных в рамках реализации мер безопасности ЗОКИИ (ИНЦ.0) [20].

Необходимо помнить о том, что субъект КИИ всегда является оператором ПДн [1], [2], [3].

Целесообразно включить в План мероприятия реагирования на КИ, связанные с обработкой ПДн субъекта КИИ в соответствии с приказами Роскомнадзора [17] и ФСБ России [8].

Инициатором разработки Плана является заместитель руководителя организации, ответственный за ИБ.

В дальнейшем он осуществляет координацию и контроль за разработкой, выполнением и актуализацией Плана [6].

Разработку Плана осуществляет подразделение по безопасности [6], [18].

Для разработки Плана должны привлекаться работники организации, обеспечивающих функционирование и эксплуатацию ЗОКИИ².

План разрабатывается в срок, не превышающий 90 календарных дней со дня включения объекта КИИ в реестр ЗОКИИ.

Разработанный План должен быть утвержден руководителем организации или уполномоченным им лицом.

После утверждения копия Плана направляется в НКЦКИ в срок до 7 календарных дней со дня его утверждения, рекомендуемый шаблон оформления письма приведен в приложении 2 к настоящим Методическим рекомендациям [13].

В случае наличия у субъекта КИИ территориально распределенных ЗОКИИ, допускается составление системы взаимоувязанных Планов.

Субъектом КИИ могут вноситься изменения в План, в том числе по результатам тренировок при отработке содержащихся в нем мероприятий, а также по результатам анализа произошедшего КИ.

При включении в План следующих разделов требуется согласование с Центром защиты информации и специальной связи ФСБ России [13]:

- Раздел 5 Условия привлечения ФСБ России»;
- Раздел 6 Порядок проведения мероприятий по реагированию совместно с ФСБ России».

Изменения в разделы 5 и 6 Плана вносятся по согласованию с ФСБ России.

Центр защиты информации и специальной связи ФСБ России рассматривает проект Плана до 30 календарных дней.

При внесении изменений План заново утверждается, а его копия в срок до 7 календарных дней со дня утверждения направляется в НКЦКИ.

Субъект КИИ при реагировании на КИ может обратиться в НКЦКИ за консультативной помощью, используя контактные данные, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет»

² К процессу согласования Плана могут быть привлечены иные лица, определенные руководителем организации или уполномоченным им лицом.

по адресу: <http://cert.gov.ru> или в рамках заключенных с НКЦКИ соглашений (регламентов) (раздел 7.5 настоящих Методических рекомендаций).

На рисунке 2 изображены общие меры по планированию мероприятий по реагированию на КИ и принятия мер по ликвидации последствий КА.



Рис. 2. Общие меры по планированию мероприятий реагирования на КИ и принятию мер по ликвидации последствий КА

5. Разделы Плана

План должен содержать перечень и состав конкретных мероприятий, проводимых субъектом КИИ на этапах «Обнаружение и регистрация КИ» и «Реагирование на КИ» в рабочее время, а также в выходные и праздничные дни, с учетом организационной структуры организации, особенностей ее информационной инфраструктуры, применяемых программных и программно-технических средств, типов КИ, их приоритетов и уровней влияния.

Пример оформления Плана приведен в приложении 3 к настоящим Методическим рекомендациям.

По структуре План содержит [13]:

5.1. Раздел 1. Технические характеристики и состав ЗОКИИ.

В данном разделе указываются:

1. Актуальные сведения о результатах категорирования ЗОКИИ (сведения о взаимодействии ЗОКИИ и сетей электросвязи, сведения о программных и программно-аппаратных средствах, используемых на ЗОКИИ) [19].

2. Сведения о наличии средств архивирования и резервного копирования данных.

3. Сведения о подключении ЗОКИИ к корпоративному (ведомственному) центру ГосСОПКА.

4. Сведения об установленных на ЗОКИИ средствах ГосСОПКА.

5.2. Раздел 2. События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий.

В данном разделе могут указываться источники информации о КИ на ЗОКИИ (программные и программно-технические средства, пользователи, администраторы, внешние источники и т.д.).

Реализация Плана начинается с момента выявления КИ на ЗОКИИ.

Источниками таких сведений могут выступать:

- сотрудники структурного подразделения субъекта КИИ, ответственного за обеспечение безопасности ЗОКИИ;

- сотрудники структурного подразделения субъекта КИИ, ответственного за эксплуатацию и (или) обеспечение функционирования ЗОКИИ, или сотрудники иной организации, выполняющие функции по эксплуатации и (или) обеспечению функционирования ЗОКИИ в силу заключенного с субъектом КИИ договора;

- сотрудники структурного подразделения субъекта КИИ, ответственного за эксплуатацию средств, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, и (или) за осуществление анализа результатов функционирования этих средств, или сотрудники иной организации, выполняющие указанные функции в силу заключенного с субъектом КИИ договора;

- сотрудники подрядных организаций, ответственные за эксплуатацию и (или) обеспечение функционирования ЗОКИИ в части заключенных договоров;

- ДИТ;

- НКЦКИ;
- Роскомнадзор;
- СМИ.

Приказом об утверждении Плана должны быть назначены должностные лица субъекта КИИ, уполномоченные на принятие решений о реализации мероприятий Плана, информирование задействованных сил (ДИТ, ОИВ, НКЦКИ и Роскомнадзор) и организацию взаимодействия с подразделениями и должностными лицами ФСБ России.

Рекомендуемая форма приказа о возложении обязанностей по реагированию на КИ и принятию мер ликвидации последствий КА на значимом объекте КИИ и об утверждении Плана приведена в приложении 4.

На рисунке 3 представлен общий подход к обнаружению и регистрации КИ, реагированию на них и информированию организации, осуществляющей координацию деятельности в части управления КИ.

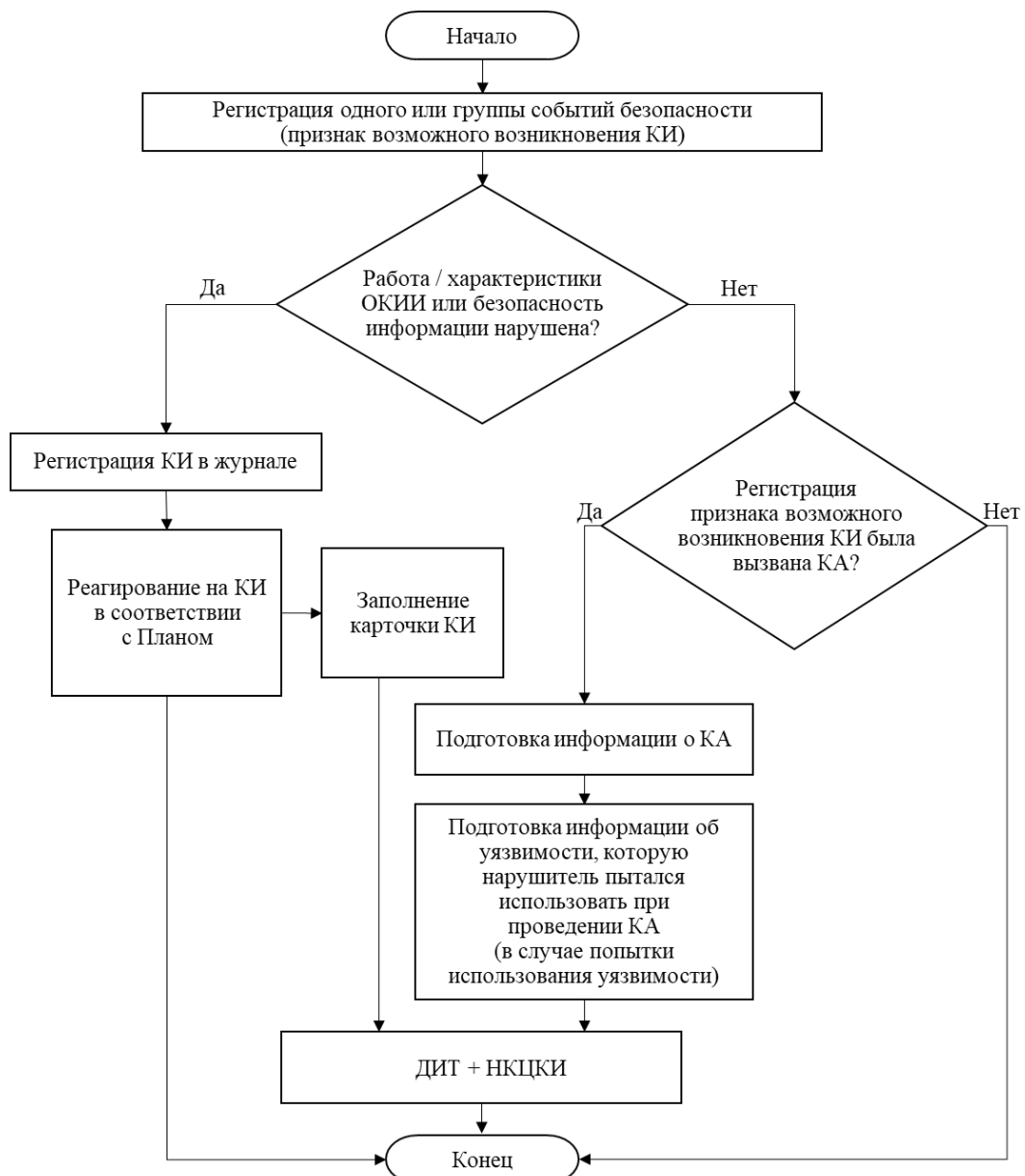


Рис. 3 Алгоритм реагирования на КИ

На рисунке 4 показан общий порядок ведения деятельности по управлению КИ.

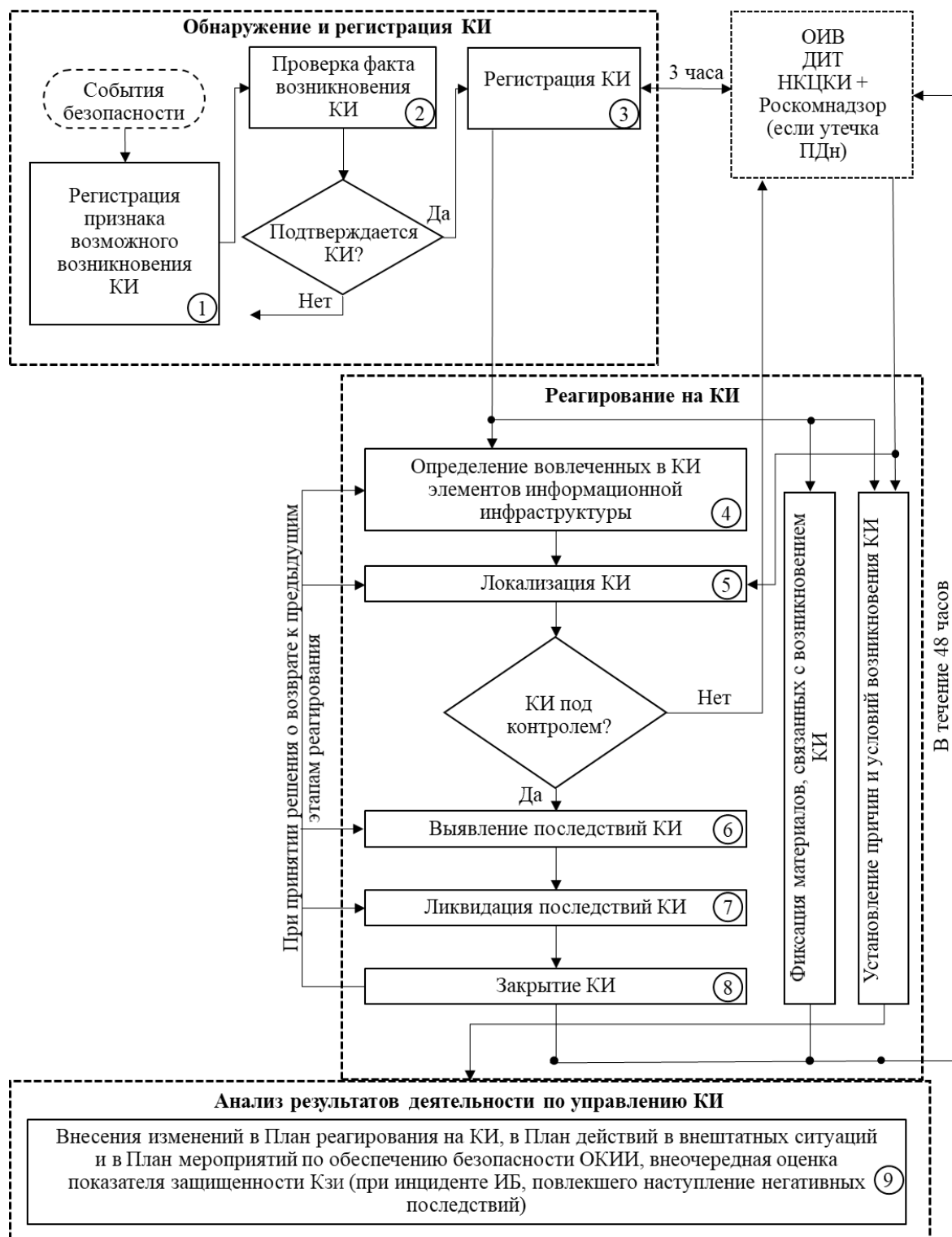


Рис. 4. Общий порядок ведения деятельности по управлению КИ

5.3. Раздел 3. Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию.

Перечень и состав конкретных мероприятий, проводимых субъектом КИИ в ходе реагирования на КИ и принятия мер по ликвидации последствий КА, разрабатывается с указанием времени, необходимых для реализации указанных мероприятий, исходя из:

- порядка предоставления сведений об инцидентах информационной безопасности [22];
- состава и особенностей функционирования элементов ЗОКИИ;
- типа выявленного компьютерного инцидента;
- состава имеющихся у субъекта КИИ сил и средств, выделенных для проведения необходимых мероприятий;
- наличия или отсутствия взаимодействия субъекта КИИ с ведомственным (корпоративным) центром ГосСОПКА;
- необходимости привлечения сил ФСБ России [13];
- положений документов, регламентирующих порядок эксплуатации ЗОКИИ и меры по обеспечению его безопасности;
- положений иных нормативных правовых актов и методических документов.

К обязательным мероприятиям реагирования относятся:

1. Обнаружение и регистрация (рекомендуемая форма карточки КИ приведена в приложении 5 к настоящим Методическим рекомендациям, рекомендуемая форма журнала учета КИ приведена в приложении 6 к настоящим Методическим рекомендациям) [13], [31], [32], [33].

2. Информирование о КИ:

– Курирующий ОИВ, ДИТ, (при необходимости поставщиков услуг (подрядчиков), ЦОД, и внешних организаций и т.д.) в установленном Порядке [18].

– НКЦКИ о КИ, связанных с ЗОКИИ, включая КИ с ПДн не позднее 3 часов с момента его обнаружения [7], [8], [13], [28].

– НКЦКИ о КИ, связанных с ОКИИ, включая КИ с ПДн не позднее 24 часов с момента его обнаружения [7], [8], [13], [28].

– Роскомнадзор о КИ с ПДн не позднее 24 часов с момента его обнаружения (первичное уведомление) [17].

3. Реагирование на КИ:

4. Определение вовлеченных в КИ элементов информационной инфраструктуры [13], [31], [32], [33].

5. Определение очередности реагирования на КИ, исходя из оценки уровня влияния КИ и приоритета [13], [31], [32], [33].

6. Локализация КИ [13], [31], [32], [33].

7. Выявление последствий КИ [13], [27], [31], [32], [33].

8. Ликвидация последствий КИ [13], [31], [32], [33].

9. Привлечение ФСБ России к ликвидации последствий КИ (при необходимости) [13], [31], [32], [33].

10. Закрытие КИ:

– Информирование НКЦКИ о результатах проведенных мероприятий не позднее 48 часов после их завершения [7], [8], [13].

– Информирование Роскомнадзор о результатах внутреннего расследования выявленного КИ с ПДн не позднее 72 часов (дополнительное уведомление) [17].

11. Анализ результатов деятельности по управлению КИ [31], [32], [33].

12. В соответствии с п.19 Методического документа [24] в случае возникновения КИ, повлекшего возникновение инцидента ИБ, повлекшего наступление негативных последствий (возникновение значимого инцидента) проводится обязательная внеочередная оценка показателя защищенности $K_{зи}$.

5.4. Раздел 4. Описание состава подразделений и должностных лиц субъекта КИИ, ответственных за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА.

Субъектом КИИ определяются подразделения и (или) должностные лица (должностное лицо), ответственные за проведение мероприятий по реагированию на КИ, связанные с функционированием ЗОКИИ.

Разрабатывается соответствующий локальный нормативный акт об определении (назначении) указанных подразделений и (или) должностных лиц (должностного лица) субъекта КИИ ответственными за данные мероприятия (приложение 4 к настоящим Методическим рекомендациям).

В Плане указываются реквизиты акта, в соответствии с которым определены (назначены) подразделения и (или) должностные лица субъекта КИИ.

При описании подразделений и должностных лиц, ответственных за проведение мероприятий Плана указываются:

– наименования подразделений субъекта КИИ, ответственных за проведение указанных мероприятий;

– ФИО, должности, контактные данные, места размещения сотрудников субъекта КИИ и возложенные на них функции по Плану.

Описание структуры сил реагирования субъекта КИИ приведено в таблице 2 [6].

Таблица 2. Распределение функций сил реагирования на КИ

Должность/подразделение	Функции
Руководитель организации	- Возлагает на заместителя руководителя организации полномочия по ИБ - Создает подразделение по ИБ - Принимает решение о привлечении внешних организаций – лицензиатов ФСТЭК России или аккредитованных ФСБ России - Несет персональную ответственность за обеспечение ИБ в организации - Принимает решение о привлечении подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ

Должность/подразделение	Функции
Заместитель руководителя организации (ответственное лицо)	- Курирует деятельность по обеспечению ИБ - Взаимодействует с ФСБ России, ФСТЭК России, ГосСОПКА (НКЦКИ), Роскомнадзор, СМИ, ОИВ, внешними и отраслевыми регуляторами, ДИТ, поставщиками услуг (подрядчиками), лицензиатами, субъектами КИИ - Отвечает за планирование и реагирование на КИ - Информировывает руководство о КИ ИБ - Руководит подразделением по ИБ - Входит в состав коллегиальных органов органа (организации)
Структурное подразделение по ИБ	- Планирование и реагирование на КИ - Выявление угроз безопасности - Предотвращение утечек информации - Обеспечение киберустойчивости - Взаимодействие с ФСБ России, ФСТЭК России, ГосСОПКА (НКЦКИ), Роскомнадзор, ОИВ, внешними и отраслевыми регуляторами, ДИТ, поставщиками услуг (подрядчиками), лицензиатами, субъектами КИИ

5.5. Раздел 5. Условия привлечения подразделений и должностных лиц ФСБ России *(при необходимости)*.

Условиями привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА являются следующие:

1. КИ привёл к прекращению функционирования ЗОКИИ.
2. Выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ, связанного с функционированием ЗОКИИ (восстановить штатное функционирование ЗОКИИ).
3. В НКЦКИ направлено сообщение о КИ, связанном с функционированием ЗОКИИ с указанием в нем необходимости привлечения подразделений и должностных лиц ФСБ России и причин, по которым выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ.

Алгоритм оценки возможности привлечения подразделений и (или) должностных лиц ФСБ России приведена на рисунке 5.

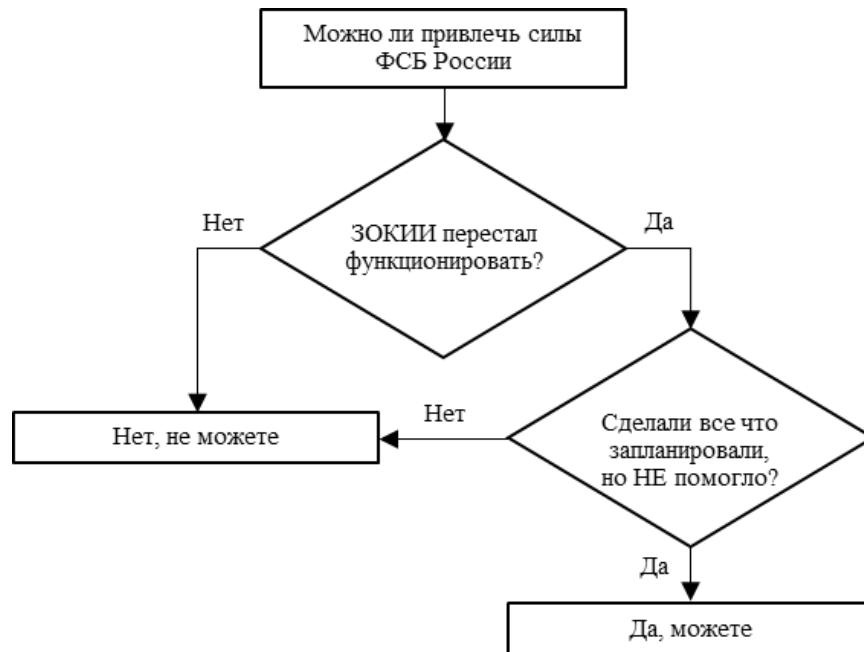


Рис. 5. Алгоритм оценки возможности привлечения подразделений и (или) должностных лиц ФСБ России

5.6. Раздел 6. Порядок проведения мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА в отношении ЗОККИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России (при необходимости).

В субъекте КИИ должно быть определено должностное лицо, ответственное за взаимодействие с подразделениями и должностными лицами ФСБ России по вопросам реагирования на КИ.

Если КИ привёл к прекращению функционирования ЗОККИ и при этом субъекту КИИ своими силами не удалось восстановить штатное функционирование ЗОККИ, то заместитель руководителя организации по вопросам ИБ, докладывает руководству субъекта КИИ о необходимости привлечения подразделений и (или) должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА.

Решение о необходимости привлечения подразделений и должностных лиц ФСБ России принимается руководством субъекта КИИ.

Для подведомственных организаций необходимо получить дополнительное согласование на привлечение подразделений и (или) должностных лиц ФСБ России от курирующего ОИВ в установленном порядке.

Ответственное лицо субъекта КИИ в течение 30 минут с момента получения указания руководства выполняет следующие действия:

1. Вносит в карточку КИ отметку о привлечении должностных лиц ФСБ России к ликвидации КА;
2. Готовит и направляет в НКЦКИ дополнительные материалы, содержащие следующие сведения:

- адрес объекта размещения вовлеченного в КИ элемента ЗОКИИ;
- контактная информация лица, сообщившего об инциденте;
- контактная информация представителей, ответственных за обеспечение функционирования вовлеченного в КИ элемента ЗОКИИ;
- время обнаружения признаков КИ;
- состав элементов ЗОКИИ, вовлеченных в КИ;
- сведения о зафиксированных нарушениях штатного режима функционирования элементов ЗОКИИ;
- сведения о предпринятых мерах;
- сведения о динамике развития КИ с учетом принятых мер;
- технические сведения о функционировании элементов ЗОКИИ (включая адреса расположения, схемы, состав, перечень используемых средств защиты информации, порядок сопряжения с внешними сетями и системами и т.д.);
- причины, по которым собственными силами ликвидация последствий КИ, связанного с функционированием ЗОКИИ, не представляется возможной.

В целях организации работы привлекаемых подразделений и должностных лиц ФСБ России выполняет следующие действия:

1. Обеспечивает беспрепятственный доступ сотрудников ФСБ России к ЗОКИИ, с функционированием которого связан КИ.
2. Обеспечивает взаимодействие сотрудников ФСБ России с уполномоченными должностными лицами субъекта КИИ.
3. Организует реализацию рекомендаций ФСБ России по ликвидации последствий КИ, повышению уровня защищенности ЗОКИИ и недопущению возникновения таких КИ в дальнейшем.

На рисунке 6 приведен алгоритм организации взаимодействия с ФСБ России при реагировании на КИ.

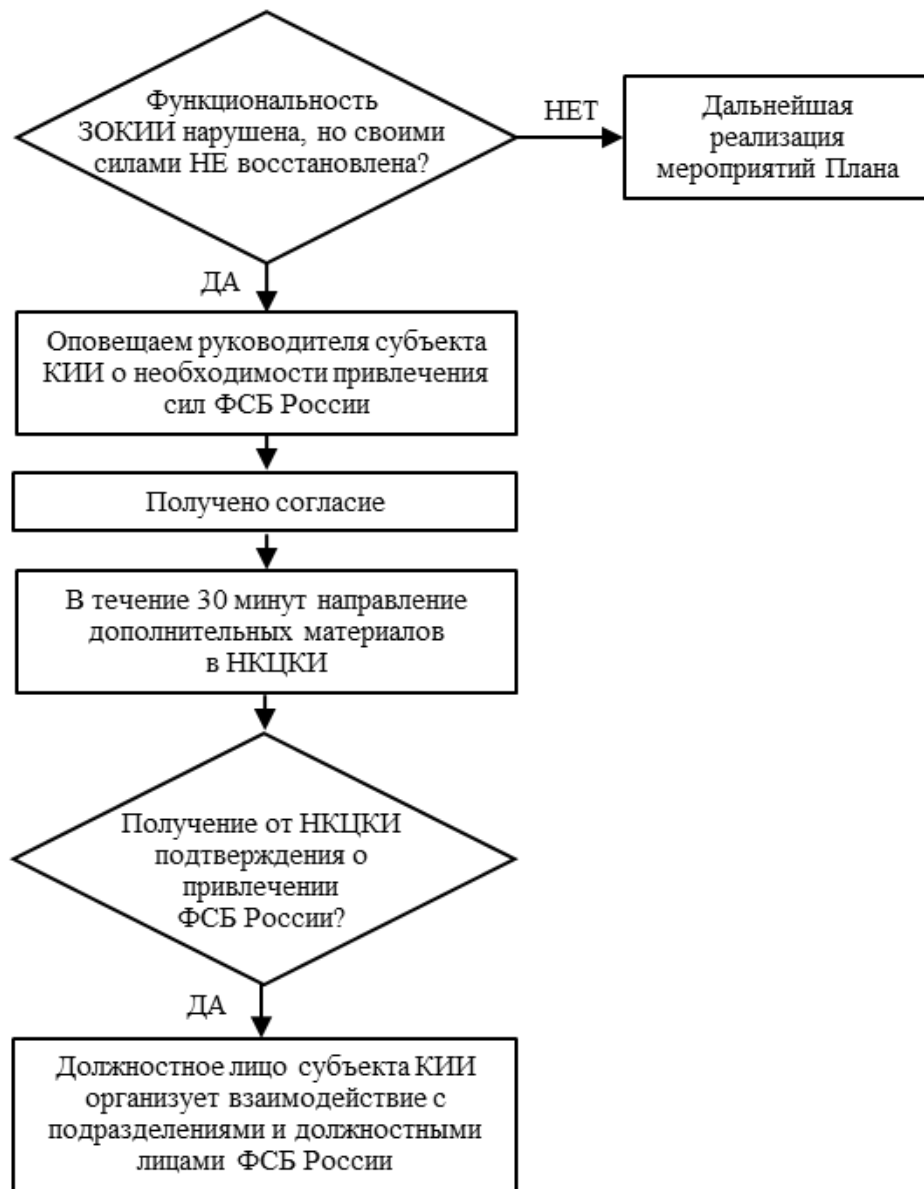


Рис. 6. Организация взаимодействия с ФСБ России при реагировании на КИ

6. Очередность реагирования на КИ

Для определения очередности мероприятий по реагированию на КИ необходимо учитывать оказываемое КИ влияние на деятельность и функционирование субъекта КИИ (приоритеты и уровни влияния) [32].

Реагирование на КИ с учетом их приоритетов и уровней влияния позволяет исключить ситуации, в которых действия по реагированию проводят в режиме «быстрая реакция», когда КИ отрабатываются в порядке их регистрации, что может привести к несвоевременному реагированию на КИ, оказывающие наибольшее негативное влияние на ЗОКИИ.

Важно отличать приоритет от уровня влияния, так как уровень влияния определяется критичностью затронутого КИ процесса, а при определении приоритета учитывают и другие критические процессы, функционирующие на тех же СВТ.

Пример анализа очередности реагирования на КИ приведен на рисунке 7.

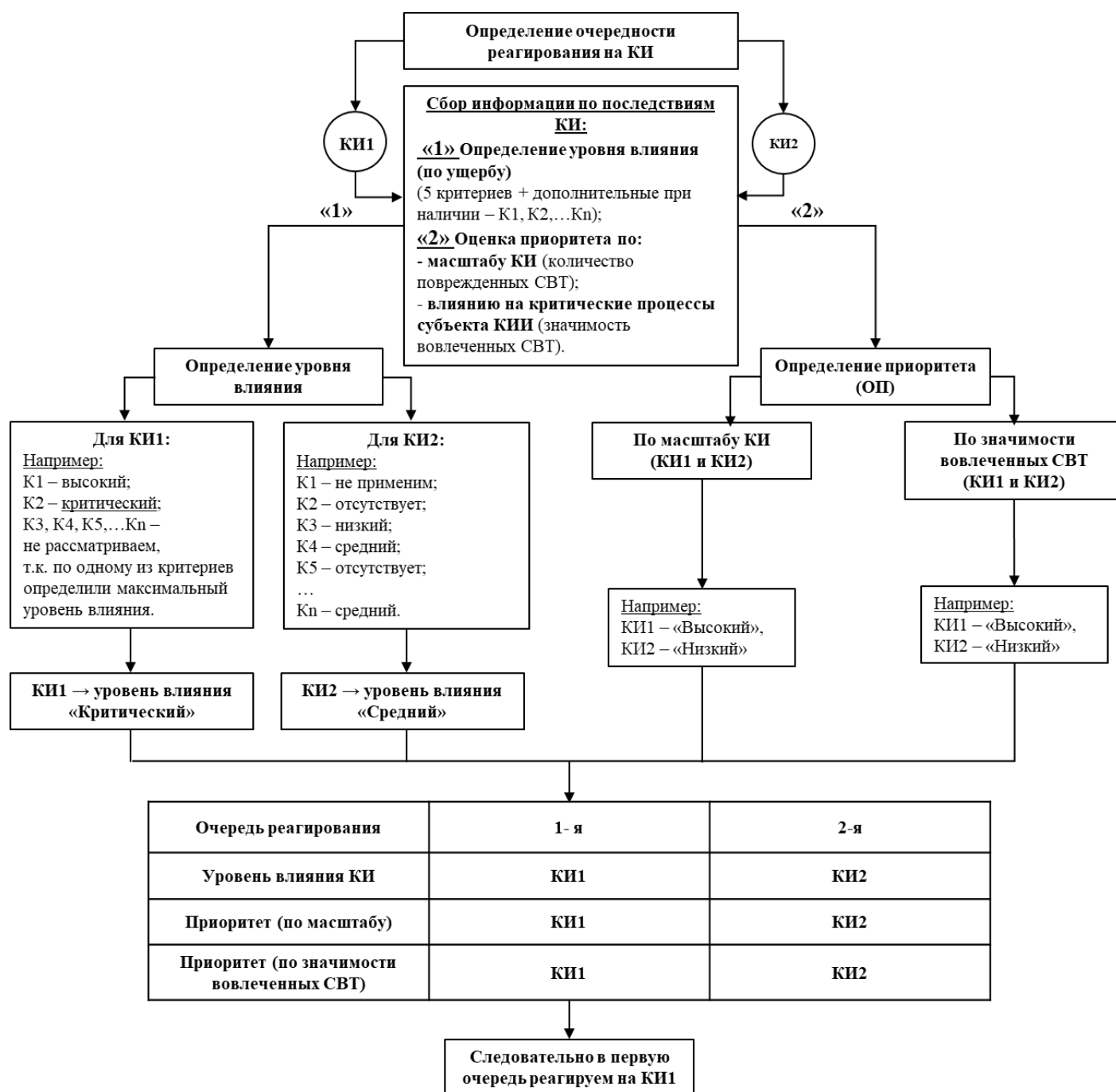


Рис.7. Пример анализа очередности реагирования на КИ

6.1. Определение уровня влияния КИ.

Подход к определению уровней влияния КИ основан на следующих критериях (К1...Кп):

- ущерб в социальной сфере (К1);
- ущерб в политической сфере (К2);
- ущерб в экономической сфере (К3);
- ущерб в экологической сфере (К4);
- ущерб для обеспечения обороны страны, безопасности государства и правопорядка (К5).

Организации могут формировать свои критерии по примеру критериев (K1...K5).

Например, связанные с экономическим ущербом, выраженным в затратах на восстановление информационных ресурсов (K_n).

По каждому критерию установлено не более четырех уровней влияния:

- критический;
- высокий;
- средний;
- низкий.

При этом допускается использовать меньшее количество уровней влияния.

Например, если по определенному критерию не может быть низкого ущерба, допускается устанавливать уровни влияния: критический, высокий и средний. Бывают и другие ситуации, когда по определенному критерию не может быть критического ущерба, в таких случаях могут быть установлены уровни влияния: высокий, средний и низкий.

В зависимости от сферы деятельности организации не все критерии будут подходить для определения уровня влияния КИ по отношению к ее информационным ресурсам. В таких случаях используются только те критерии, которые подходят для конкретной организации и ее информационных ресурсов.

Итоговый уровень влияния КИ оценивается как максимальный уровень влияния среди определенных по разным критериям.

В случае если по какому-либо критерию зафиксирован максимальный уровень влияния, то дальнейшее определение уровней влияния прекращается и присваивается итоговый уровень влияния «Критический»

Определение итогового уровня влияния на КИ приведено на рисунке 8.

Подход к определению уровней влияния приведен в приложении 7 к настоящим Методическим рекомендациям [32].

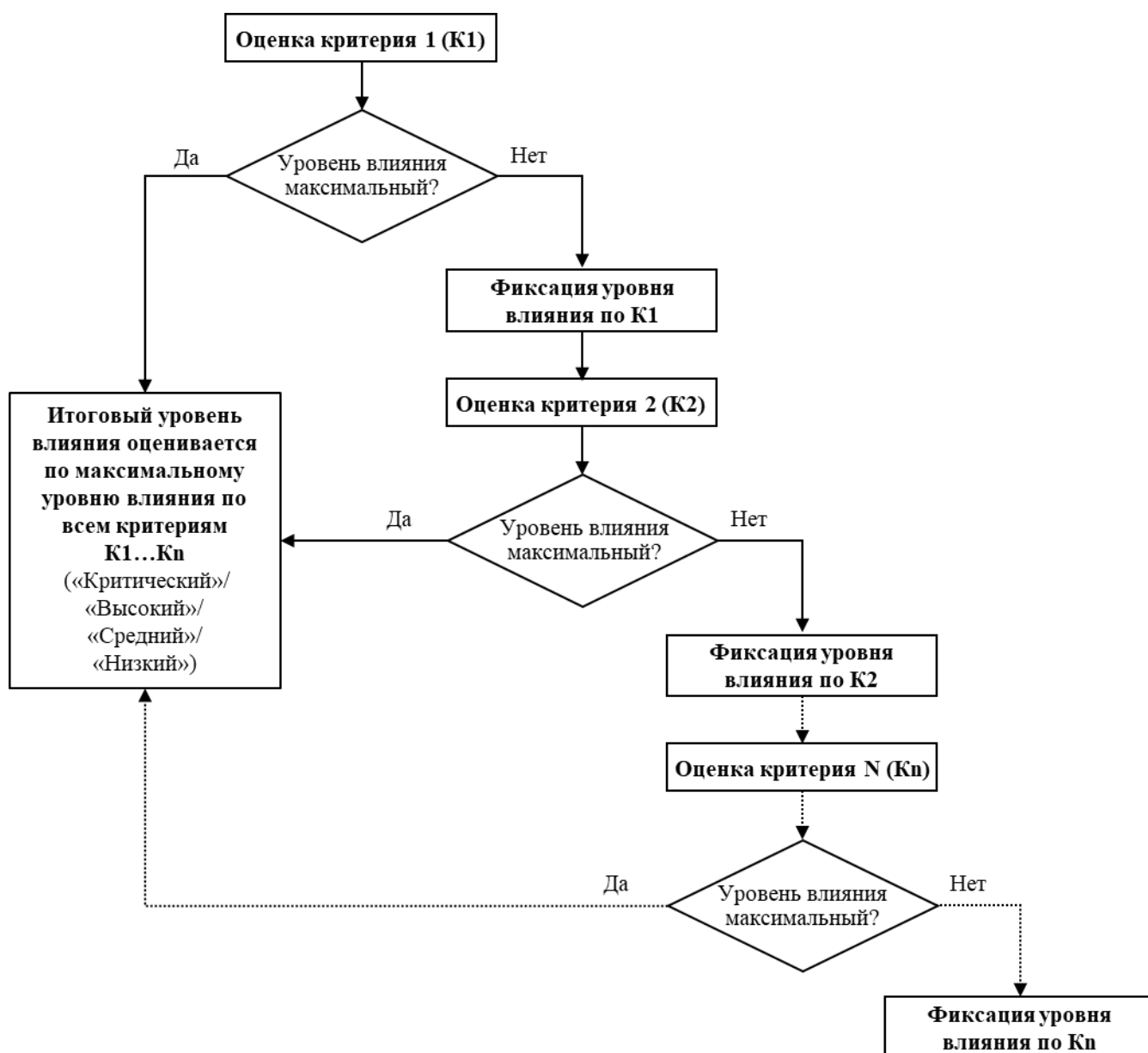


Рис.8. Определение итогового уровня влияния на КИ

6.2. Определение приоритетов КИ и очередности реагирования на КИ.

При определении приоритетов используются следующие критерии КИ:

- масштаб КИ (пример приведен в таблице 3);
- значимость СВТ, на которых обнаружены признаки данного КИ (пример приведен в таблице 4).

Таблица 3. Определение приоритета: масштаб КИ

Приоритет	Количество СВТ, на которых обнаружены признаки зарегистрированного КИ
Высокий	30% и более
Средний	10% - 30%
Низкий	10%

Таблица 4. Определение приоритета: значимость вовлеченных СВТ

Приоритет	Значимость вовлеченных СВТ
Высокий	СВТ, реализующие сервисы, связанные с критическими процессами
Средний	СВТ, с которых КИ наиболее быстро может распространиться на СВТ, связанные с критическими процессами
Низкий	Иные СВТ

Возможно использовать дополнительные критерии при оценке приоритета. По каждому критерию установлено не более трех приоритетов:

- высокий;
- средний;
- низкий.

Итоговый приоритет КИ оценивают как максимальный приоритет среди определенных по разным критериям. В случае если по какому-либо критерию зафиксирован максимальный приоритет, то дальнейшая оценка приоритетов прекращается и присваивается итоговый максимальный приоритет.

Например, если по критерию «значимость элементов ЗОКИИ» приоритет КИ определен как «Средний», а по критерию «масштаб КИ» как «Низкий», то итоговый приоритет КИ определяют как «Средний».

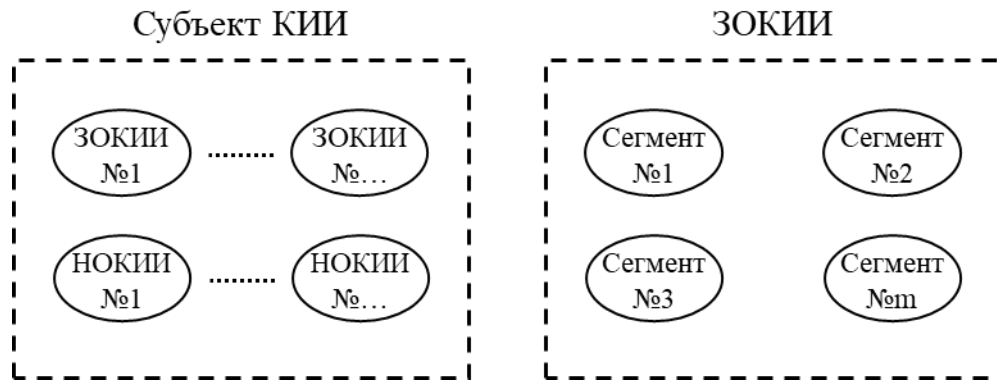
Приоритеты не зависят от уровней влияния КИ и могут использоваться совместно с ними для определения очередности обработки КИ.

Порядок определения очередности реагирования на КИ приведен в таблице 5:

Таблица 5. Порядок определения очередности реагирования на КИ

Очередь реагирования	1-я	2-я	3-я	4-я	5-я	6-я	7-я	8-я	9-я
Уровень влияния компьютерного инцидента	Критический	Высокий	Высокий	Средний	Средний	Средний	Низкий	Низкий	Низкий
Приоритет компьютерного инцидента	Высокий	Высокий	Средний	Высокий	Средний	Низкий	Высокий	Средний	Низкий

Допускается разработка единого Плана на все ЗОКИИ субъекта КИИ, а также разработка отдельных Планов в отношении отдельных сегментов ЗОКИИ. (рисунок 9).



**Рис. 9. (Слева) Общее количество ЗОКИИ у субъекта КИИ,
(Справа) Разбивка ЗОКИИ на отдельные сегменты**

При разработке единого Плана на все ОКИИ субъекта КИИ необходимо включить раздел об оценке приоритетов, а также определить ответственное лицо за расстановку приоритетов при реагировании на КИ.

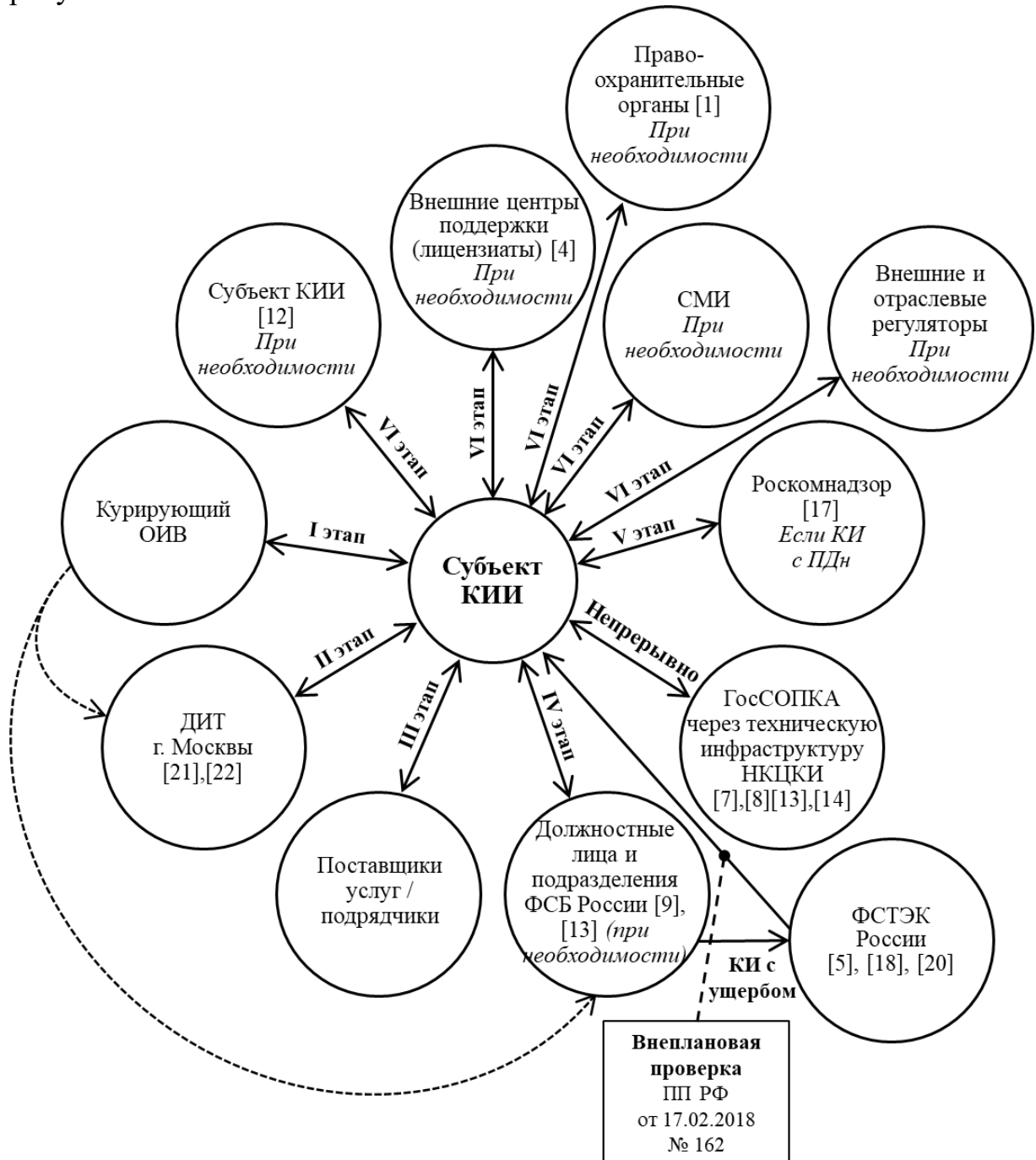
При наличии отдельных Планов оценка приоритетов, определяется регламентом с назначением ответственного лица субъекта КИИ.

В соответствии с данным показателем приоритет КИ определяют в зависимости от значимости СВТ, на которых обнаружены признаки данного КИ. Значимость СВТ определяют в зависимости от функционирующих на данном СВТ сервисов, содержащейся на нем информации и (или) возможности распространения КИ на более значимые СВТ.

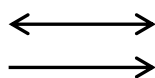
7. Организация взаимодействия

В рамках реагирования на КИ и принятия мер по ликвидации последствий КА субъект КИИ взаимодействует со следующими органами государственной власти и организациями.

Взаимодействие субъекта КИИ при реагировании на КИ представлено на рисунке 10.



Условные обозначения на рисунке:



Двустороннее взаимодействие

Одностороннее взаимодействие

Рис. 10. Взаимодействие субъекта КИИ при реагировании на КИ

7.1. Взаимодействие с подразделениями внутри организации.

В организации должно быть организовано взаимодействие подразделения и (или) должностных лиц (должностного лица), ответственных за проведение мероприятий по реагированию на КИ, связанных с функционированием ЗОКИИ, со смежными подразделениями, также участвующими в деятельности по управлению КИ.

Должны быть определены способы взаимодействия, правила и процедуры, в рамках которых такое взаимодействие будет реализовано [31].

Подразделение, ответственное за управление КИ, в ходе своей деятельности может взаимодействовать со следующими специалистами:

- подразделения, ответственного за эксплуатацию ЗОКИИ;
- подразделениями субъекта КИИ, ответственного за эксплуатацию и (или) обеспечение функционирования ЗОКИИ;
- юридического подразделения;
- отдела кадров;
- отдела по связям с общественностью;
- подразделений обеспечения безопасности организации.

В организации должен быть регламентирован порядок взаимодействия подразделений, включая разделение функций и полномочий в случае возникновения КИ (утвержден приказом по организации).

Специалисты юридического подразделения должны предоставлять рекомендации и консультации по вопросам соблюдения требований законодательства РФ в ходе деятельности по управлению КИ.

Специалисты отдела кадров должны принимать участие в процедурах привлечения к дисциплинарной ответственности работников организации, уличенных в действиях, которых привели к КИ.

Специалисты отдела по связям с общественностью должны быть готовы обрабатывать любые запросы СМИ и оказывать содействие в разработке политик и процедур раскрытия информации.

7.2. Взаимодействие субъекта КИИ с курирующим ОИВ.

Порядок взаимодействия субъекта КИИ с курирующим ОИВ должен быть регламентирован внутренним локальным нормативным актом.

Информирование ДИТ осуществляется по установленной форме, посредством электронной почты: dit_incident@mos.ru [22].

7.3. Взаимодействие с поставщиками услуг (подрядчиками).

Субъекты КИИ при реагировании на компьютерный инцидент взаимодействуют с поставщиками услуг (подрядчиками) в рамках договора на оказание работ (услуг).

7.4. Взаимодействие с ФСБ России.

Взаимодействие осуществляется в соответствии с разделом 6 Плана (при необходимости) или по инициативе ФСБ России.

7.4.1. Взаимодействие при КИ в период проведения ФСБ России оценки защищенности³.

Условия, при которых субъект КИИ при КИ начинает взаимодействие с ФСБ России, являются следующими [9]:

1. ОКИИ имеет непосредственное подключение к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») и (или) сопряженных с сетью «Интернет» с использованием технологии трансляции сетевых адресов.

2. Получение уведомления от ФСБ России субъекту КИИ о включении его в План проведения оценки защищенности информационных ресурсов.

3. Получение уведомления от ФСБ России субъекту КИИ за 14 дней до начала проведения мероприятий по оценке защищенности информационных ресурсов.

Приказом организации должны быть назначены должностные лица, уполномоченные осуществлять взаимодействие с подразделениями и должностными лицами ФСБ России в период проведения ФСБ России оценки защищенности.

Необходимость включения в План дополнительного раздела о взаимодействии субъекта КИИ с ФСБ России при КИ в период проведения ФСБ России оценки защищенности определяется исходя из наличия подключения объекта КИИ к сети «Интернет».

Пример заполнения данного раздела Плана приведен в приложении 8 к настоящим Методическим рекомендациям.

Алгоритм определения источника возникновения КИ при проведении ФСБ России оценки защищенности информационных ресурсов приведен на рисунке 11.

Алгоритм взаимодействия с ФСБ России при проведении ФСБ России оценки защищенности информационных ресурсов приведен на рисунке 12.

³ Аналогичная процедура оценки защищенности информационных ресурсов при взаимодействии с Центром защиты информации и специальной связи Федеральной службы безопасности Российской Федерации.

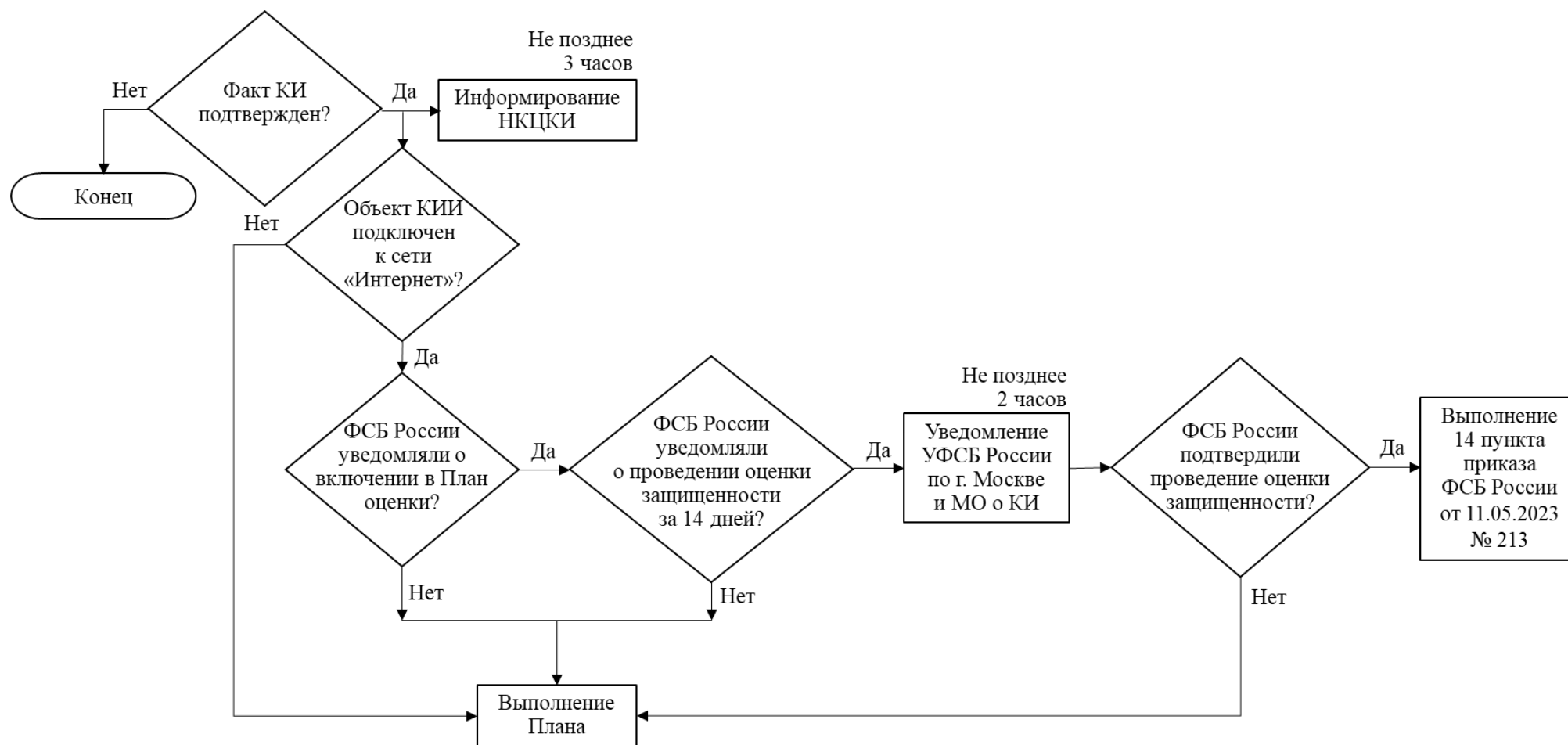


Рис.11. Определение источника возникновения КИ при проведении ФСБ России оценки защищенности

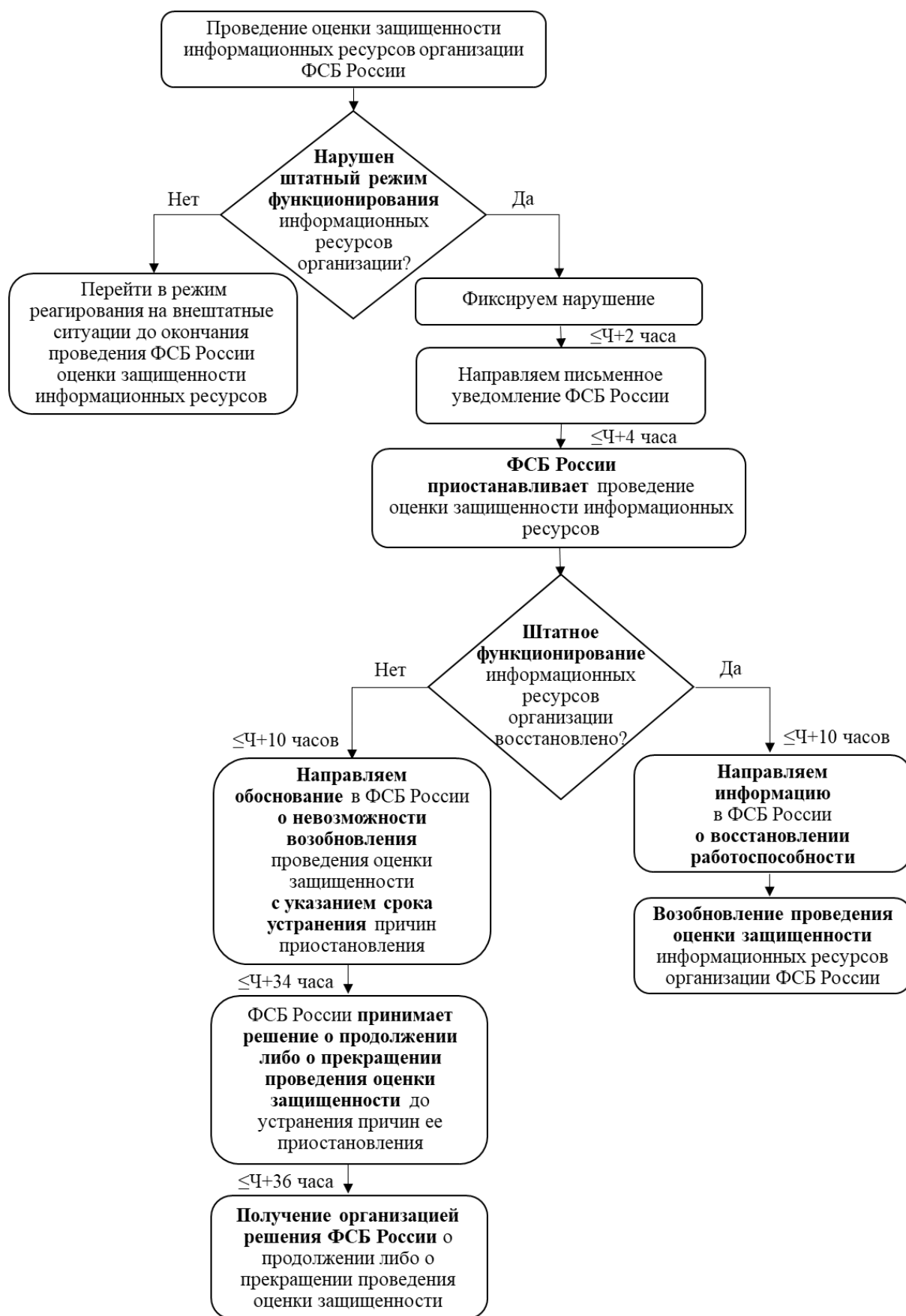


Рис.12. Алгоритм взаимодействия с ФСБ России при проведении ФСБ России оценки защищенности информационных ресурсов

7.5. Взаимодействие в ГосСОПКА и НКЦКИ.

Каждый субъект КИИ обязан подключиться к технической инфраструктуре НКЦКИ (порядок подключения приведен [на портале ГосСОПКА](#)). Для объектов ЗОКИИ взаимодействие с ГосСОПКА осуществляется непрерывно.

В соответствии с пунктом 3 приказа ФСБ России [14] субъекты КИИ обязаны:

- направлять информацию о КА и КИ;
- получать информацию об угрозах безопасности информации, в том числе о готовящихся КА и признаках КИ, связанных с функционированием ЗОКИИ.

Взаимодействие осуществляется посредством личного кабинета субъекта ГосСОПКА (далее — личный кабинет). При отсутствии связи или техническом сбое информация о КА и КИ направляется по резервным каналам связи, указанным в личном кабинете.

Взаимодействие субъектов КИИ с ГосСОПКА в рамках информирования о КИ, реагирования на них и принятия мер по ликвидации последствий КА осуществляется в соответствии с приказом ФСБ России [7], а о КИ, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн осуществляется в соответствии с приказом ФСБ России [8].

Варианты организации взаимодействия с ГосСОПКА[14]:

1. Силами структурного подразделения, ответственного за обеспечение ИБ, с заключением соглашения (издания совместного акта) о взаимодействии с ФСБ России (НКЦКИ), включающего в том числе права и обязанности сторон, порядок проведения совместных мероприятий, регламент информационного обмена, порядок и сроки представления отчетности, порядок и формы контроля.

2. Силами структурного подразделения, ответственного за обеспечение информационной безопасности, с его аккредитацией как центра ГосСОПКА.

3. Силами организаций, являющихся аккредитованными центрами ГосСОПКА.

Каналы обмена информацией с НКЦКИ организованы следующими способами:

- подключение к технической инфраструктуре НКЦКИ через личный кабинет;
- напрямую с НКЦКИ [11], для этого субъекту КИИ необходимо:

Изучить [регламент взаимодействия](#) [29] и [Методические рекомендации по организации прямого взаимодействия с НКЦКИ](#) [25].

Также на сайте НКЦКИ создан [электронный сервис для помощи в формировании уведомлений о КА и КИ](#) (рисунок 13).

В зависимости от выбранного типа события информационной безопасности в данной форме могут появляться дополнительные разделы для обязательного заполнения (например, если инцидент связан с утечкой ПДн, то в данной форме дополнительно появится раздел «Сведения об утечке ПДн» (рисунок 14).

Сформированное уведомление необходимо направить в НКЦКИ на адрес электронной почты incident@cert.gov.ru.

– По вопросам организации взаимодействия с НКЦКИ: info@cert.gov.ru, телефон: +7 (916) 901-07-42.

– По вопросам подключения к технической инфраструктуре НКЦКИ: network@cert.gov.ru +7 (495) 621-10-68.

– Почтовый адрес: 107031, г. Москва, ул. Большая Лубянка, д. 1/3.

Форма составления уведомления об атаке или инциденте

Данная форма предназначена для помощи субъектам КИИ и иным владельцам российских информационных ресурсов в составлении уведомления в адрес НКЦКИ. После заполнения формы сформированное уведомление необходимо направить на адрес электронной почты incident@cert.gov.ru

Категория

Выберите категорию уведомления

Тип события ИБ

Тип события ИБ

Общие сведения

Заявитель, например: ОАО «Компания»

Краткое описание

Сведения о средстве или способе выявления

Статус реагирования

Необходимость привлечения сил ГосСОПКА

Ограничительный маркер TLP

Влияние на конфиденциальность

Влияние на целостность

Влияние на доступность

Утечка ПДн

Краткое описание иной формы последствий компьютерного инцидента

Дата и время выявления (Дата/время UTC+0)

дд-мм-гггг --:--

Дата и время завершения (Дата/время UTC+0)

дд-мм-гггг --:--

Общие сведения о контролируемом ресурсе

Наименование

Информация о категорировании ОКИИ

Сфера функционирования

Наличие подключения к сети Интернет

Местоположение контролируемого ресурса

Локация

Населенный пункт или геокоординаты

Сформировать

Рис.13. Форма составления уведомления об атаке или компьютерном инциденте

Сведения об утечке персональных данных

ИНН

Полное наименование

Адрес оператора

Адрес электронной почты для отправки информации об уведомлении

Предполагаемые причины, повлекшие нарушение прав субъектов ПД

Характеристики персональных данных

Предполагаемый вред, нанесенный правам субъектов ПД

Принятые меры по устранению последствий инцидента

Дополнительный сведения

Информация о результатах внутреннего расследования инцидента

Сформировать

Рис.14. Форма (на сайте НКЦКИ) для формирования сведений об утечке ПДн

7.6. Взаимодействия с Роскомнадзором.

В соответствии с приказом [17] оператор обязан сообщать в Роскомнадзор информацию о произошедшем инциденте с ПДн.

В течение 24 часов после происшествия информирует об инциденте, предполагаемом вреде субъекту ПДн, а также о должностном лице, уполномоченном на взаимодействие с Роскомнадзором по данному инциденту.

Через 72 часа оператор сообщает о результатах внутреннего расследования выявленного инцидента.

Взаимодействие с Роскомнадзором осуществляется с использованием портала Госуслуг.

Оператору необходима подтвержденная учетная запись на Госуслугах, привязанная к личному кабинету организации для информирования Роскомнадзора.

Алгоритмы взаимодействия операторов ПДн с ГосСОПКА и Роскомнадзором при возникновении инцидента с ПДн приведены на рисунках 15 и 16.

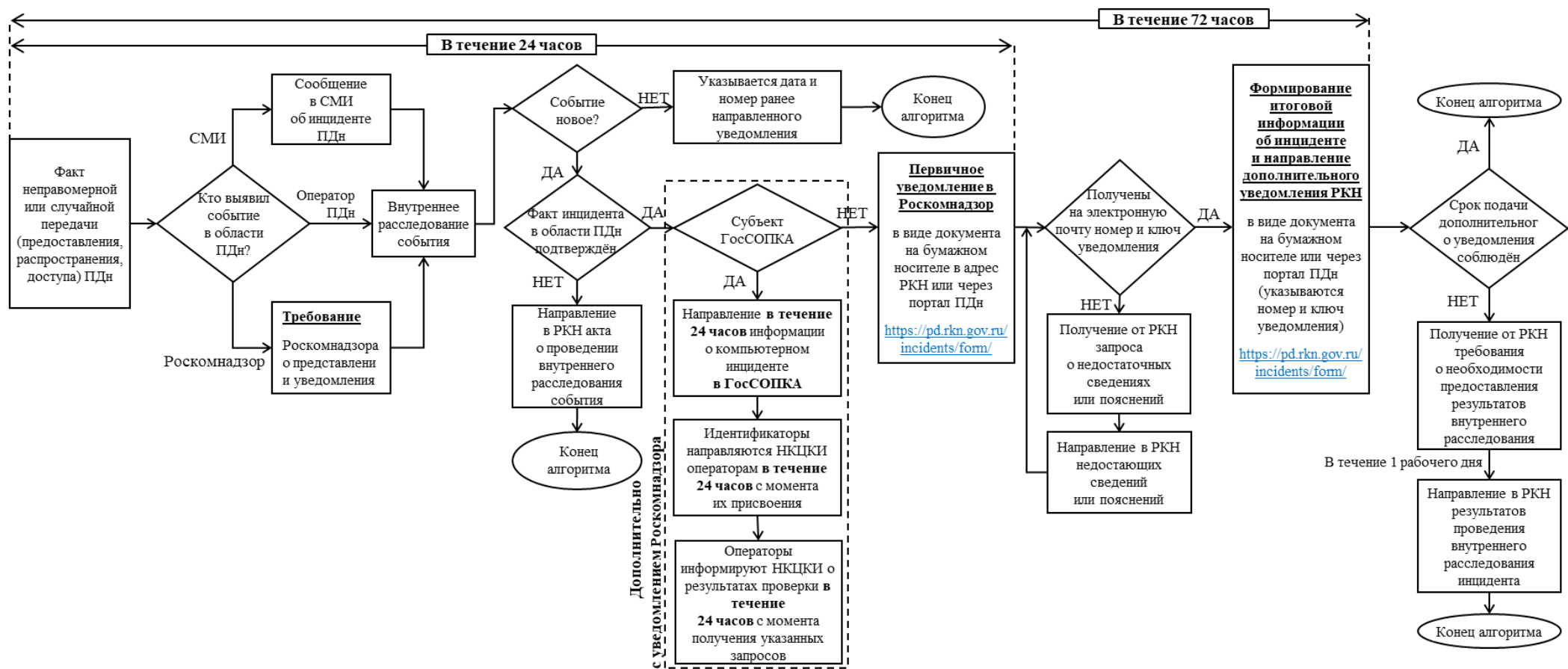


Рис.15. Алгоритм взаимодействия операторов ПДн с ГосСОПКА и РКН при возникновении инцидента с ПДн

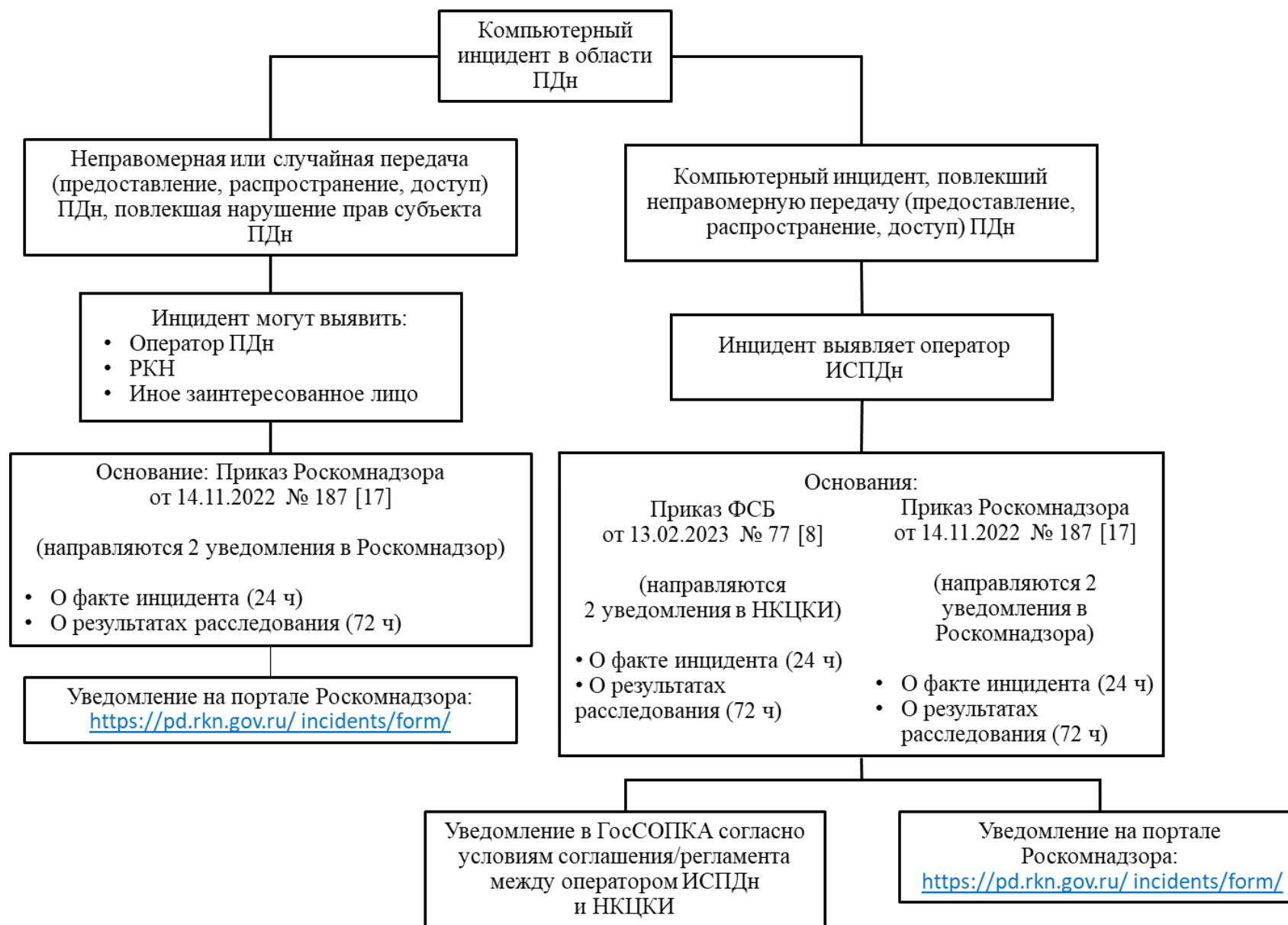


Рис. 16. Алгоритм взаимодействия операторов ПДн с ГосСОПКА и Роскомнадзором при возникновении инцидента с ПДн

7.7. Взаимодействие со ФСТЭК России.

В соответствии с подпунктом «б» пункта 20 Постановления Правительства Российской Федерации от 17.02.2018 № 162 [5] возникновение КИ на значимом объекте КИИ, повлекшего негативные последствия является основанием для осуществления внеплановой проверки ФСТЭК России субъекта КИИ,

ФСТЭК России вправе приступить к проведению внеплановой проверки субъекта КИИ незамедлительно, если компьютерный инцидент повлек негативные последствия.

В случае если на субъект КИИ распространяются требования по обеспечению готовности к объявлению уровня опасности целевых КА, необходимо учитывать и увязывать План (Планы) с Планом действий при введении соответствующего уровня целевых КА.

В случае возникновения КИ на значимом объекте КИИ, повлекшим наступление негативных последствий, субъект КИИ проводит обязательную внеочередную оценку показателя защищенности $K_{зи}$ в соответствии с п. 18 Методических рекомендаций «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [24].

7.8. Взаимодействие с другими субъектами КИИ.

Правила обмена информацией о компьютерных инцидентах между субъектами КИИ, между субъектами КИИ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты утверждены приказом ФСБ России от 25.12.2025 № 546 [12].

7.9. Взаимодействие с лицензиатами и внешними центрами поддержки.

В соответствии с подпунктом «в» пункта 1 Указа Президента Российской Федерации от 01.05.2022 № 250 [4] для осуществления мероприятий по обеспечению информационной безопасности в случае необходимости кредитные организации могут принимать решения о привлечении организаций. При этом могут привлекаться исключительно организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации.

Субъектам КИИ необходимо провести инвентаризацию договоров с подрядными организациями, оказывающими услуги по информационной безопасности. Учитывать это требование нужно и при принятии дальнейших решений о привлечении подрядчиков.

Реестр лицензиатов ФСТЭК России размещён на официальном сайте регулирующего органа в открытом доступе (электронный адрес: <https://reestr.fstec.ru/reg1>).

7.10. Взаимодействие с внешними и отраслевыми регуляторами.

В связи с созданием отраслевых центров информационной безопасности при ФОИВ (Минцифры России, Минпромторг России, Минэнерго России,

Минтранс России и т.д.) необходимо учитывать возможность взаимодействия субъекта КИИ с ними.

7.11. Взаимодействие с правоохранительными органами.

КИ на ЗОКИИ может служить основанием для возбуждения уголовного дела по ст. 274.1 УК РФ [1]. В связи с этим необходимо учесть в Плане мероприятия по взаимодействию с правоохранительными органами в рамках проведения оперативно-розыскных мероприятий.

Предусмотреть обеспечение бесперебойного функционирования ЗОКИИ в случае изъятия компонентов ЗОКИИ для проведения компьютерно-технических экспертиз.

Обеспечить сохранение «цифровых доказательств» при аварийно-восстановительных работах.

7.12. Взаимодействие со СМИ.

В случае если КИ привел к нарушению жизнедеятельности городского хозяйства, в том числе прекращению оказания Государственных услуг города Москвы, необходимо предусмотреть мероприятия по информированию населения и предотвращению распространения панических и недостоверных сведений в СМИ и социальных сетях.

8. Средства реагирования

Для эффективной реализации запланированных Планом мероприятий должны быть предусмотрены средства, предназначенные для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, в том числе к средствам, предназначенным для поиска признаков компьютерных атак (далее – средства реагирования).

Требования к средствам реагирования изложены в приказе ФСБ России [16].

Каждый исполнитель, указанный в Плате, должен быть обеспечен всеми необходимыми средствами реагирования, списком контактов, иметь план коммуникаций в случае возникновения КИ, знать места размещения ЗОКИИ и/или его сегментов, особенность доступа к ним (пропуска, наряды допуски, наличие индивидуальных средств защиты и т.д.).

Алгоритм проверки обеспеченности средствами реагирования и готовности к их использованию приведен на рисунке 17.

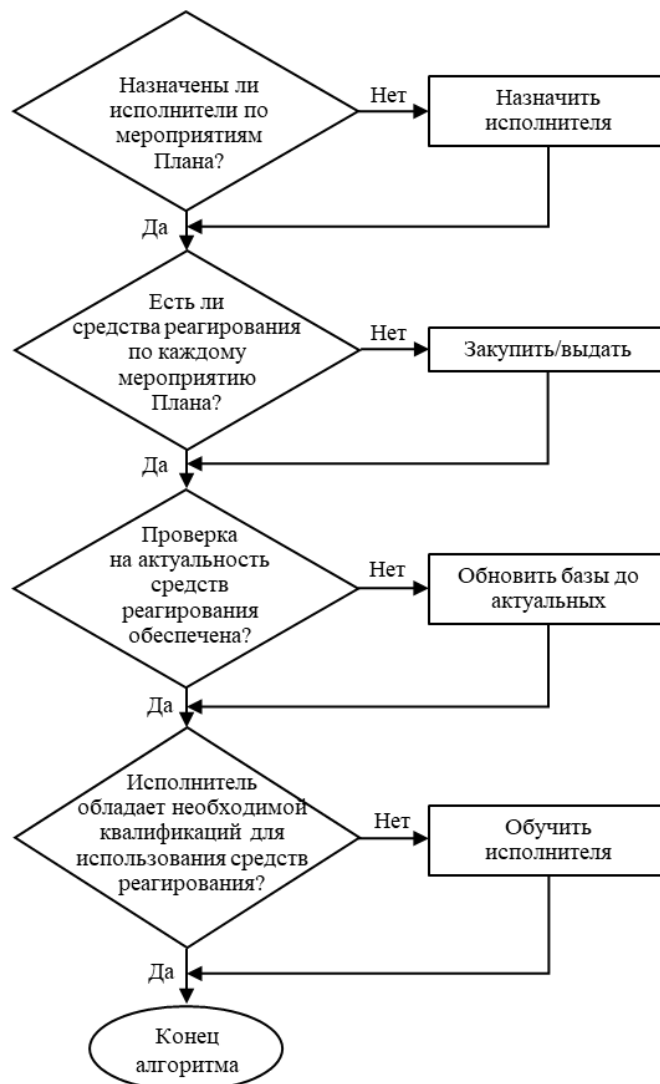


Рис. 17. Алгоритм проверки обеспеченности средствами реагирования и готовности к их использованию

В таблице 6 приведен примерный список средств реагирования, который при их необходимости указывается в Плате для каждого отдельного мероприятия.

Таблица 6. Список средств реагирования

№ п/п	Средства реагирования	Обоснование применения
1.	Флеш-накопитель	Перенос информации
2.	Дистрибутивы средств защиты информации	Восстановление работоспособности
3.	Образы ПО	Восстановление работоспособности
4.	Портативный мобильный роутер	Резервный доступ в интернет для обновления баз данных
5.	Инструмент (отвертки, гаечные ключи и т.д.)	Демонтаж/монтаж оборудования из аппаратной стойки
6.	ПАК СЗИ	Восстановление работоспособности
7.	Запасное имущество и принадлежности (ЗИП)	Восстановление работоспособности

Приведенный пример в таблице 6 является базовым и неокончательным.

Исполнитель по данному мероприятию Плате должен обладать достаточной квалификацией для эффективного использования выделенными средствами реагирования при ликвидации последствий КИ.

9. Обеспечение процессов реагирования

Для реализации запланированных Планом мероприятий должны быть предусмотрены средства, обеспечивающие процессы реагирования на КИ.

В таблице 7 приведен примерный список средств, обеспечивающих процессы реагирования на КИ и обоснование их применения, которые при необходимости указываются в Плате для каждого отдельного мероприятия.

Таблица 7. Список средств, обеспечивающих процессы реагирования на КИ

№ п/п	Средства, обеспечивающие процессы реагирования	Обоснование применения
1.	Доставка к месту КИ служебным транспортом	Доставка сил реагирования, ЗИП и т.д. к месту размещения ОКИИ
2.	Индивидуальные средства защиты	Требования по охране труда
3.	Организация пропускного режима	При привлечении сил ДИТ, ОИВ, ФСБ России
4.	Пропуск на внос/вынос материальных средств	Для служебных целей
5.	Тележка для перевозки грузов	Для служебных целей
6.	Средства автономного энергоснабжения	При централизованном отключении электроснабжения.
7.	Резервный интернет-канал	При невозможности подключения по основному каналу

Приведенный пример в таблице 7 является базовым и неокончательным.

Планом должно быть определено время выполнения каждого мероприятия с учетом времени прибытия исполнителя к местам размещения ЗОКИИ.

10. Маркеры (вехи) при выполнении этапов Плана

Планом должны быть четко определены маркеры (вехи), отделяющие конец одного этапа от начала другого.

Образец заполнения маркеров (вех) при выполнении этапов Плана приведен в приложении 9.

11. Порядок действий, разработанный ФСТЭК России, по обеспечению безопасности объектов КИИ и технической защиты информации в органах государственной власти и организациях при реализации угроз безопасности информации

ФСТЭК России⁴ рекомендовал использовать Порядок действий по обеспечению безопасности объектов КИИ и технической защиты информации в органах государственной власти и организациях при реализации угроз безопасности информации (далее – Порядок).

Порядок типа «отказ в обслуживании» приведен в приложении 10.

Порядок, связанный с внедрением нежелательного контента на информационном ресурсе приведен в приложении 11.

Порядок, связанный с несанкционированным доступом к защищаемой информации приведен в приложении 12.

Порядок, связанный с внедрением вирусов-шифровальщиков приведен в приложении 13.

Выполнение указанных Порядков не должен противоречить и (или) отменять порядок действий по реагированию на компьютерные атаки, установленный нормативно-правовыми актами ФСБ России.

⁴ Письмо ФСТЭК России от 30.07.2024 № 240/93/3514.

12. Заключение

Просим направлять замечания и предложения к настоящим Методическим рекомендациям по разработке Плана реагирования на КИ и принятия мер по ликвидации последствий КА, проведенных в отношении ЗОКИИ в адрес начальника отдела обеспечения осведомленности Комарова В.В. (KomarovVV@it.mos.ru).

Приложение 1
к Методическим рекомендациям

**Рекомендуемый шаблон сопроводительного письма о направлении на
согласование проекта Плана реагирования на КИ и принятия мер
по ликвидации последствий КА в адрес ФСБ России**

**Центр защиты информации и
специальной связи ФСБ России**

В соответствии с пунктом 8 приказа ФСБ России от 25.12.2025 № 547 «Об утверждении Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» направляем на согласование проект Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак в отношении значимого объекта критической информационной инфраструктуры «Наименование».

Приложение: по тексту на ___ л. в 1 экз.

Должность

И.О.Фамилия

Приложение 2
к Методическим рекомендациям

**Рекомендуемый шаблон сопроводительного письма о направлении копии
Плана реагирования на КИ и принятия мер по ликвидации последствий КА в
адрес НКЦКИ**

**Директору Национального
координационного центра по
компьютерным инцидентам
О.В.Скрябину
Большая Лубянка ул., д.1/3,
Москва, 107031
info@cert.gov.ru**

Уважаемый Олег Валерьевич!

В соответствии с пунктом 6 приказа ФСБ России от 25.12.2025 № 547 «Об утверждении Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» направляем в Ваш адрес копию утвержденного плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак в отношении значимого объекта критической информационной инфраструктуры «Наименование».

Приложение: по тексту на ___ л. в 1 экз.

Должность

И.О.Фамилия

Приложение 3
к Методическим рекомендациям

**Пример оформления Плана реагирования на КИ
и принятия мер по ликвидации последствий КА**

Раздел 1. Технические характеристики и состав ЗОКИИ

Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи		
1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Отсутствует взаимодействие ЗОКИИ с сетью связи общего пользования, а также наложенными или выделенными сетями. Объект расположен локально в пределах инженерного сооружения.
2.	Наименование оператора связи и (или) провайдера хостинга	Отсутствует
3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Отсутствует
4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	Отсутствует
Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры		
1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного	- CA-7200, DIU-N4, CA-ШУЗ, - APM 11th Gen Intel(R) Core(TM) i5-1135G7, 2.40GHz, 1.38 GHz (8 шт.)

	оборудования, средств беспроводного доступа, иных средств) и их количество	
2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии))	Windows 10 PRO
3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	FIRE 1
4.	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	Встроенные общесистемные прикладные средства, сертификация и экспертиза средств информации не производилась.
Иные сведения		
1.	Сведения о наличии средств архивирования и резервного копирования данных	Отсутствуют
2.	Сведения о подключении ЗОКИИ к корпоративному (ведомственному) центру ГосСОПКА	С центрами ГосСОПКА не взаимодействует
3.	Сведения об установленных на ЗОКИИ средствах ГосСОПКА	Средства ГосСОПКА отсутствуют

Состав значимого объекта КИИ «Наименование системы»

№ п/п	Наименование элемента значимого объекта КИИ	Сетевое имя	Провайдер	Доменное имя	Внешний IP-адрес	Внутренний IP-адрес	Используемые протоколы	ОС ⁵	ППО ⁶	Название учетных записей	Лицо, ответственное за эксплуатацию ⁷	Лицо, ответственное за администрирование	Средства защиты
1.	Коммутатор (модель)	hp	ООО «Связь»	-	-	X.X.X.X	tcp, udp, snmp, ssh	-	-	admin			
2.	Сервер (модель)	serv	-	-	-	X.X.X.X	tcp, udp, ssh	ОС (наименование, версия)	ППО (наименование, версия)	User1-User8			АВС ⁸ (наименование, версия)
3.	СВТ (модель)	User1	-	-	-	X.X.X.X	tcp, udp	ОС (наименование, версия)	ППО (наименование, версия)	User1			АВС (наименование, версия)
4.	СВТ (модель)	User2	-	-	-	X.X.X.X	tcp, udp	ОС (наименование, версия)	ППО (наименование, версия)	User2			АВС (наименование, версия)
5.	СВТ (модель)	User3	-	-	-	X.X.X.X	tcp, udp	ОС (наименование, версия)	ППО (наименование, версия)	User3			АВС (наименование, версия)

⁵ Операционная система.

⁶ Прикладное программное обеспечение.

⁷ Указывается номер строки из Раздела 4 настоящего приложения, в которой содержатся сведения о соответствующем должностном лице.

⁸ Антивирусное средство.

									версия)				
6.	СВТ (модель)	User4	-	-	-	X.X.X.X	tcp, udp	ОС (наименование, версия)	ППО (наименование, версия)	User4			АВС (наименование, версия)
7.	СВТ (модель)	User5	-	-	-	X.X.X.X	tcp, udp	ОС (наименование, версия)	ППО (наименование, версия)	User5			АВС (наименование, версия)
8.	СВТ (модель)	User6	-	-	-	X.X.X.X	tcp, udp	ОС (наименование, версия)	ППО (наименование, версия)	User6			АВС (наименование, версия)
8.	СВТ (модель)	User7	-	-	-	X.X.X.X	tcp, udp	ОС (наименование, версия)	ППО (наименование, версия)	User7			АВС (наименование, версия)
9.	СВТ (модель)	User8	-	-	-	X.X.X.X	tcp, udp	ОС (наименование, версия)	ППО (наименование, версия)	User8			АВС (наименование, версия)

Раздел 2. События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий

Замедление, временный сбой или прекращение работы АРМ, сервисов и иных компонентов ЗОКИИ;

Нарушение установленного в организации режима доступа к информации или компонентам ЗОКИИ;

Функционирование ВПО;

Несанкционированное изменение информации на элементах ЗОКИИ;

Превышение допустимой нагрузки на вычислительные ресурсы элементов ЗОКИИ;

Отказ функционирующего на элементах ЗОКИИ программного и аппаратного обеспечения;

Иные нарушения в работе элементов ЗОКИИ, вызывающих прекращение выполнения его целевых функций.

Источники информации о КИ на ЗОКИИ

СЗИ:

Сбор и первичная обработка событий, связанных с нарушением информационной безопасности (далее — события ИБ), осуществляется из следующих источников:

- операционных систем серверов и автоматизированных рабочих мест;
- средств и систем защиты информации ЗОКИИ/ОКИИ, включая оповещения и уведомления;
- систем мониторинга, в том числе средств обнаружения вторжений;
- межсетевых экранов;
- средств предотвращения утечек данных;
- антивирусного ПО;
- телекоммуникационного оборудования, систем мониторинга его состояния, средств управления им и сетями связи;
- прикладных сервисов;
- средств контроля (анализа) защищенности;
- систем мониторинга качества обслуживания;
- журналов событий ПО АСУ ТП;
- систем резервного копирования и других систем;
- средств автоматического или автоматизированного мониторинга информационной безопасности учреждения.

Пользовательские, административные и внешние источники информации:

Сотрудники учреждения, ответственные за ИБ: куратор ИБ, ответственный за ИБ участка, администратор, старший диспетчер, диспетчер (оператор АСУ), начальник дежурной смены, пользователи;

Уведомления или информирование ДИТ;

Уведомления или информирование ФСТЭК России или НКЦКИ информацию об угрозах безопасности информации, в том числе о готовящихся компьютерных атаках и признаках компьютерных инцидентов, связанных с функционированием ЗОКИИ [10], [14];

СМИ.

**Раздел 3. Мероприятия, проводимые в ходе реагирования
на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время,
отводимое на их реализацию**

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последоват ельность	Результат	Примечание
12.2. Обнаружение и регистрация КИ								
1.1.	Незамедлительный доклад начальнику дежурной смены о произошедшем КИ	Устный доклад	Диспетчер (оператор АСУ)	Начальник дежурной смены	Ч + 5 мин.			
1.2.	Заполнение карточки КИ	Карточка, распечатанная на бумаге, ручка / АРМ (форма в электронной форме)	Диспетчер (оператор АСУ)	Начальник дежурной смены	Ч + 10 мин.	После выполнения п. 1.1	В карточку внесена запись о КИ	
1.3.	Заполнение журнала КИ	Оформленный по форме журнал, ручка	Диспетчер (оператор АСУ)	Начальник дежурной смены	Ч + 15 мин.	После выполнения п. 1.2	В журнал внесена запись о КИ	
1.4.	Незамедлительное информирование ответственного лица, уполномоченного предоставлять сведения о КИ в ДИТ, НКЦКИ о произошедшем КИ (старшего диспетчера)	Устный доклад	Начальник дежурной смены	Ответственное лицо, уполномоченное предоставлять сведения о КИ в ДИТ, НКЦКИ о произошедшем КИ Старший диспетчер службы ИТС	Ч + 10 мин.	После выполнения п. 1.3		
1.5.	Незамедлительное информирование ответственного за ИБ участка и	Устный доклад	Начальник дежурной смены	Старший диспетчер службы ИТС	Ч + 15 мин.	После выполнения п. 1.4		

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	администратора о произошедшем КИ							
1.6.	Незамедлительное информирование куратора ИБ участка о произошедшем КИ	Устный доклад	Ответственный за ИБ участка	Куратор ИБ	Ч + 20 мин.	После выполнения п. 1.5		
1.7.	Незамедлительное информирование заместителя руководителя организации по вопросам ИБ о произошедшем КИ	Устный доклад	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 25 мин.	После выполнения п. 1.6		
1.8.	Направление дежурной бригады на место размещения ЗОКИИ для выяснения обстоятельств, приведших к ошибке/сбою	Служебный транспорт, необходимый инструмент (отвертки, гаечные ключи и т.д.), дистрибутивы СЗИ, запасное имущество и принадлежности (ЗИП)	Начальник дежурной смены	Куратор ИБ	Ч + 25 мин.	После выполнения п. 1.7		Служебный транспорт
12.3. Определение вовлеченных в КИ элементов информационной инфраструктуры								
2.1.	Сбор сообщений от технических средств	Общесистемное ПО, АВЗ.	Ответственный за ИБ участка	Куратор ИБ	Ч + 25 мин.	После выполнения п. 1.6		
2.2.	Сбор сообщений от работников, пользователей,	Опрос / получение письменных объяснений	Куратор ИБ	Заместитель руководителя	Ч + 30 мин.	После выполнения п. 1.7		

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	привилегированных пользователей			организации по вопросам ИБ				
2.3.	Сбор доказательств	Журналы регистрации событий, копий жестких дисков и других данных, собранных на предшествующих этапах и т.п.	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 35 мин.	После выполнения п 2.2		
2.4.	Сбор сведений об уязвимостях, посредством которых были реализованы угрозы ИБ	Сканер уязвимостей	Ответственный за ИБ участка	Куратор ИБ	Ч + 30 мин.	После выполнения п 2.1	Зафиксированное свидетельство	
2.5.	Сбор данных, зафиксированных системами контроля доступа и видеонаблюдения		Ответственный за ИБ участка	Куратор ИБ	Ч + 40 мин.	После выполнения п 2.4		
12.4. Определение очередности реагирования на КИ								
3.1.	Определение очередности реагирования на КИ, исходя из оценки уровня влияния КИ и приоритета	Сбор информации по последствиям КИ, определение уровня влияния и приоритетов (по масштабу и по значимости вовлеченных СВТ	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 50 мин.	После выполнения п 2.3	Решение заместителя руководителя последовательности мероприятий по результатам определения	

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
							очередности реагирования	
12.5. Локализация КИ								
4.1.	Направление ответственного за ИБ для проведения диагностических работ по выявлению и локализации КИ	Служебный транспорт, флеш-накопитель, дистрибутивы СЗИ, образы ПО и т.д.	Ответственный за ИБ участка	Куратор ИБ	Ч + 60 мин.	После выполнения п 2.5		
4.2.	Отключение пораженных элементов ЗОКИИ		Ответственный за ИБ участка	Куратор ИБ	Ч + 60 мин.	После выполнения п 4.1		
4.3.	Блокировка скомпрометированных учетных записей	АРМ	Ответственный за ИБ участка	Куратор ИБ	Ч + 1 ч. 05 мин.	После выполнения п 4.2		
4.4.	Изъятие съемных носителей	Жесткий диск, флеш-накопитель	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 60 мин.	После выполнения п 3.1		
4.5.	Визуальный осмотр мест размещения ЗОКИИ на предмет выявления и фиксации попыток несанкционированной установки ПО, установки внешних носителей информации, нарушения опломбирования, нарушения	ПАК СЗИ для выявления КИ	Ответственный за ИБ участка	Куратор ИБ	Ч + 1 ч. 20 мин.	После выполнения п 4.3		

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	целостности кабельной инфраструктуры и иных нарушений информационной безопасности ЗОКИИ/ОКИИ и его компонентов							
4.6.	Мониторинг и фиксация попыток несанкционированной установки ПО, установки внешних носителей информации и иных действий, проводимых на оборудовании, АРМ и серверах, входящих в периметр ЗОКИИ/ОКИИ.	ПАК СЗИ для выявления КИ	Ответственный за ИБ участка	Куратор ИБ	Ч + 1 ч. 50 мин.	После выполнения п 4.5		
4.7.	Передача данных о проведенных работах по локализации КИ, диспетчеру (оператору АСУ) для дальнейшего информирования старшего диспетчера,	Устный доклад/ телефон/ электронная почта	Ответственный за ИБ участка	Куратор ИБ	Ч + 2 ч. 30 мин.	После выполнения п 4.6		

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	куратора ИБ и заместителя руководителя организации по вопросам ИБ							
4.8.	Протоколирование действий по локализации	АРМ	Старший диспетчер	Куратор ИБ	Ч + 2 часа 40 мин.	После выполнения п. 4.7		
12.6. Информирование курирующего ОИВ, ДИТ, НКЦКИ, поставщиков услуг (подрядчиков) и внешних организаций								
5.1.	Уведомление курирующего ОИВ о КИ	Телефон/ электронная почта	Старший диспетчер	Куратор ИБ	Ч + 30 мин.	После выполнения п. 1.7		
5.2.	Уведомление ДИТ о КИ (посредством электронной почты:)	Электронная почта: dit_incident@mos.ru	Старший диспетчер	Куратор ИБ	Ч + 40 мин.	После выполнения п. 5.1		
5.3.	Информирование внешних организаций о компрометации ключей электронной подписи	Электронная почта, телефон	Старший диспетчер	Куратор ИБ	Ч + 50 мин.	После выполнения п. 5.2		
5.4.	Уведомление поставщиков услуг (подрядчиков)	Телефон/ электронная почта	Старший диспетчер	Куратор ИБ	Ч + 60 мин.	После выполнения п. 5.3		
5.5.	Уведомление НКЦКИ о КИ	Личный кабинет субъекта ГосСОПКА	Старший диспетчер	Куратор ИБ	Ч + 3 ч.	После выполнения п. 4.9		
5.6.	Доведение сведений о проведенных мероприятиях по информированию	Личный доклад	Старший диспетчер	Куратор ИБ	Ч + 3 ч. 10 мин.	После выполнения п. 5.6		

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	куратора ИБ и заместителя руководителя организации по вопросам ИБ							
12.7. Выявление последствий КИ								
6.1.	Выявление работоспособности СВТ		Ответственный за ИБ участка	Куратор ИБ	Ч + 3 ч. 30 мин.	После выполнения п. 4.7		
6.2.	Протоколирование выявленных последствий	АРМ	Старший диспетчер	Куратор ИБ	Ч + 4 ч.	После выполнения п. 6.1	Внесение данных в протокол	
12.8. Ликвидация последствий КИ								
7.1.	Использование всех возможных мер по восстановлению работоспособности ЗОКИИ	АРМ, загрузка антивируса, обновление ПО и смена скомпрометированных паролей, восстановление данных из резервных копий, удаление вредоносного кода, восстановление настройки технических средств, связанности элементов ЗОКИИ, Проведение	Ответственный за ИБ участка	Куратор ИБ	Ч + 4 ч. 30 мин.	После выполнения п. 6.1		

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
		нагрузочного тестирования т.д.						
7.2.	Протоколирование действий по ликвидации последствий КИ	АРМ	Старший диспетчер	Куратор ИБ	Ч + 4 ч. 45 мин.	После выполнения п. 7.1	Внесение данных в протокол	
7.3.	Доклад о произведенных работах по ликвидации последствий КИ старшему диспетчеру, куратору ИБ и заместителю руководителя организации по вопросам ИБ	Личный доклад	Старший диспетчер	Куратор ИБ	Ч + 5 ч.	После выполнения п. 7.2		
12.9. Привлечение ФСБ России к ликвидации последствий КИ								
8.1.	Решение о привлечении ФСБ России, если работоспособность ЗОКИИ не восстановлена	Устное решение	Заместитель руководителя организации по вопросам ИБ		Ч + 6 ч.	После выполнения п. 7.3	Устное решение	
8.2.	Внесение в журнал отметки об информировании НКЦКИ о необходимости привлечения	Журнал, ручка	Старший диспетчер	Куратор ИБ	Ч + 6 ч. 10 мин.	После выполнения п. 8.1		

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	должностных лиц ФСБ России							
8.3.	Направление в НКЦКИ дополнительных материалов	Личный кабинет субъекта ГосСОПКА	Старший диспетчер	Куратор ИБ	Ч + 6 ч. 30 мин.	После выполнения п. 8.2		
8.4.	Получение от НКЦКИ подтверждения о привлечении ФСБ России	Электронная почта, телефон	Старший диспетчер	Куратор ИБ	Ч + 8 ч.	После выполнения п. 8.3		
8.5.	Организация взаимодействия с подразделениями и должностными лицами ФСБ России	Пропуск к ЗОКИИ, АРМ	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 10 ч.	После выполнения п. 8.4		Обеспечение прохода на территорию, предоставление должностным лицам ФСБ России АРМов, и точек входа для подключения к ЗОКИИ со служебного ноутбука
12.10.Заккрытие КИ								
9.1.	Издание приказа о проведении расследования	Приказ, согласованный и подписанный в установленном порядке	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 30 ч.	После выполнения п. 8.5		

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
9.2.	Проведение расследования КИ, выявление причин возникновения и оценивание нанесённого ущерба КИ ЗОКИИ	Просмотр и обработка лог-файлов АРМ, записей видеокамер внутреннего наблюдения, данных СКУД и других имеющихся технических и административных возможностей учреждения, не противоречащих действующему законодательству, изучение объяснительных, служебных записок от персонала	Ответственный за ИБ участка	Куратор ИБ	Ч + 30 ч. 30 мин.	После выполнения п. 9.1	Проект акта по результатам проведённого расследования КИ, причины возникновения, условия и обстоятельства КИ	
9.3.	Информирование заместителя руководителя организации по вопросам ИБ о проведенном расследовании	Устный доклад	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 35 ч. 30 мин.	После выполнения п. 9.2		
9.4.	Подписание акта по результатам проведённого расследования КИ	Оформленный акт	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 36 ч.	После выполнения п. 9.3	Подписанный акт по результатам проведённого	

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
							расследования КИ	
9.5.	Информирование ДИТ, ОИВ о результатах расследования КИ и о нанесенном ущербе КИ	Электронная почта: dit_incident@mos.ru	Старший диспетчер	Куратор ИБ	Ч + 36 ч. 20 мин.	После выполнения п. 9.4		
9.6.	Информирование ЦОДД о закрытии КИ	Электронная почта, телефон	Старший диспетчер	Куратор ИБ	Ч + 36 ч. 50 мин.	После выполнения п. 9.5		
9.7.	Направление в НКЦКИ результатов расследования КИ	Личный кабинет субъекта ГосСОПКА	Старший диспетчер	Куратор ИБ	Ч + 48 ч.	После выполнения п. 9.6		
9.8.	Внесение журнал КИ о времени оповещения НКЦКИ о результатах расследования КИ	Журнал, ручка / АРМ	Диспетчер (оператор АСУ)	Куратор ИБ	Ч + 48 ч. 30 мин.	После выполнения п. 9.7		
12.11. Анализ результатов деятельности по управлению КИ [23], [27]								
10.1.	Разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения КИ	Рекомендации по принятию дополнительных мер защиты информации в соответствии с нормативными правовыми актами и методическими документами уполномоченных федеральных	Куратор ИБ, ответственный за ИБ участка / администратор, старший диспетчер, начальник дежурной смены	Заместитель руководителя организации по вопросам ИБ	Ч + 7 дней	После выполнения п. 9.8	Рекомендации доложены руководителю	При необходимости по решению руководства

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последоват ельность	Результат	Примечание
		органов исполнительной власти (ФСБ России и ФСТЭК России), в том числе доработку (актуализацию) и/или разработку документации, регламентирующей вопросы обеспечения безопасности организации; рекомендации по повышению защищенности информационных ресурсов от компьютерных атак; рекомендации по устранению технических причин и условий, способствующих проведению деструктивного воздействия на информационные ресурсы.						

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
10.2.	Оценка результатов и эффективности реагирования на КИ, предусмотренная Планом	Оценка достаточности и эффективности процессов и процедур реагирования на компьютерные инциденты, изложенных в Плане; предложения по включению в План дополнительных процессов и процедур, которые могли бы повысить эффективность действий, выполняемых на стадиях «обнаружение и регистрация КИ» и «реагирование на КИ»; предложения по использованию дополнительных инструментальных средств с целью повышения эффективности реагирования и	Куратор ИБ, ответственный за ИБ участка / администратор, старший диспетчер, начальник дежурной смены	Заместитель руководителя организации по вопросам ИБ	Ч + 10 дней	После выполнения п. 10.1	Рабочее совещание проведено	При необходимости и по решению руководства

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
		установления причин и условий возникновения КИ; оценка эффективности обмена информацией о КИ между всеми сторонами, принимающими участие на стадиях «обнаружение и регистрация КИ» и «реагирование на КИ».						
10.3.	Внесение изменений в План реагирования на КИ и принятия мер по ликвидации последствий КА и его утверждение	АРМ, План	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 14 дней	После выполнения п. 10.2		При необходимости и по решению руководства
10.4.	Отправка проекта Плана реагирования на КИ и принятия мер по ликвидации последствий КА на согласование в ФСБ России	Проект Плана, письмо в ФСБ	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 16 дней	После выполнения п. 10.3		Если в Плане задействованы силы ФСБ России
10.5.	Доработка проекта Плана реагирования на КИ и принятия	Проект Плана, письмо в ФСБ	Куратор ИБ	Заместитель руководителя	Ч + 20 дней	После выполнения п. 10.4		Если требуется внести

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последоват ельность	Результат	Примечание
	мер по ликвидации последствий КА с учетом мнения ФСБ России			организации по вопросам ИБ				изменения по результатам согласования
10.6.	Утверждение Плана реагирования на КИ и принятия мер по ликвидации последствий КА	План	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 25 дней	После выполнения п. 10.5		
10.7.	Направление копии измененного Плана реагирования на КИ и принятия мер по ликвидации последствий КА в НКЦКИ	Копия утвержденного Плана	Куратор ИБ	Заместитель руководителя организации по вопросам ИБ	Ч + 32 дня	После выполнения п. 10.6		

Раздел 4. Подразделения и должностные лица, ответственные за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА

№ п/п	Ответственное лицо (ФИО) / должность	Роль	Контактные данные	Адрес электронной почты	Адрес и место размещения (номер кабинета)	Реквизиты приказа (распоряжения)
1.	ФИО, руководитель организации	Возлагает на заместителя руководителя организации полномочия по ИБ Создает подразделение по ИБ Принимает решение о привлечении подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ	Телефоны: - рабочий, - мобильный	xxx@mos.ru		Приказ (распоряжение) от XX.XX.XXXX № XXX
2.	ФИО, заместитель руководителя организации по вопросам ИБ	Курирует деятельность по обеспечению ИБ Взаимодействует с ФСБ России, ФСТЭК России, ГосСОПКА (НКЦКИ), РКН, СМИ, ОИВ, внешними и отраслевыми регуляторами, ДИТ, поставщиками услуг (подрядчиками), лицензиатами, субъектами КИИ при проведении мероприятий по реагированию на КИ Информирует руководство о КИ Руководит структурным подразделением по ИБ Получает информацию о КИ на ЗОКИИ/ОКИИ от начальника структурного подразделения по ИБ	Телефоны: - рабочий, - мобильный	xxx@mos.ru		Приказ (распоряжение) от XX.XX.XXXX № XXX

№ п/п	Ответственное лицо (ФИО) / должность	Роль	Контактные данные	Адрес электронной почты	Адрес и место размещения (номер кабинета)	Реквизиты приказа (распоряжения)
3.	ФИО, куратор ИБ	Получает информацию о КИ на ЗОКИИ от ответственного за ИБ. Передаёт поступившую информацию заместителю руководителя организации по вопросам ИБ. Совместно с Ответственным за ИБ проводит расследование произошедшего КИ на ЗОКИИ. Координирует работу и действия Участников процесса. Осуществляет выработку рекомендаций/проведение мероприятий (совместно с Ответственным за ИБ) по недопущению КИ на ЗОКИИ в будущем.	Телефоны: - рабочий, - мобильный	xxx@mos.ru		Приказ (распоряжение) от XX.XX.XXXX № XXX
4.	ФИО, начальник дежурной смены	Осуществляет общее руководство и контроль за действиями дежурной смены во время её дежурства. При потере автоматизированного управления и мониторинга параметров ЗОКИИ/ОКИИ, направляет дежурную бригаду для включения управления в «ручном/местном».	Телефоны: - рабочий, - мобильный	xxx@mos.ru		Приказ (распоряжение) от XX.XX.XXXX № XXX

№ п/п	Ответственное лицо (ФИО) / должность	Роль	Контактные данные	Адрес электронной почты	Адрес и место размещения (номер кабинета)	Реквизиты приказа (распоряжения)
5.	ФИО, старший диспетчер	Получает информацию от Диспетчера (оператора АСУ) о КИ на ЗОКИИ. Регистрирует КИ в общем Журнале КИ. Передаёт поступившую информацию в НКЦКИ, ДИТ, курирующий ОИВ, ЦОДД. Получает сообщения, рекомендации и предписания от НКЦКИ. Передаёт поступившую информацию от НКЦКИ Диспетчеру (оператору АСУ). Вносит данные о КИ в журнал учёта КИ. Протоколирование действий.	Телефоны: - рабочий, - мобильный	xxx@mos.ru		Приказ (распоряжение) от XX.XX.XXXX № XXX
6.	ФИО, диспетчер (оператор АСУ)	Фиксирует невозможность автоматизированного управления, контроля и мониторинга параметров ЗОКИИ, в результате сбоя/неисправности в работе ЗОКИИ. Докладывает о произошедшем начальнику дежурной смены. Заполняет карточку КИ. Направляет регистрационную форму КИ Старшему диспетчеру. Регистрирует КИ в Журнале учёта КИ. Получает уведомления и инструкции НКЦКИ от старшего диспетчера.	Телефоны: - рабочий, - мобильный	xxx@mos.ru		Приказ (распоряжение) от XX.XX.XXXX № XXX

№ п/п	Ответственное лицо (ФИО) / должность	Роль	Контактные данные	Адрес электронной почты	Адрес и место размещения (номер кабинета)	Реквизиты приказа (распоряжения)
		Участвует в мероприятиях по выявлению и реагированию на КИ ЗОКИИ ⁹ .				
7.	ФИО, ответственный за ИБ участка	Проводит предварительную проверку состояния ИБ ЗОКИИ. Участвует в мероприятиях по реагированию КИ ЗОКИИ. Передаёт данные о КИ (пункт №4 Карточки КИ), на бумажном носителе или посредством служебной электронной почты Диспетчеру (оператору АСУ). Передаёт информацию о произошедшем КИ старшему дежурному смены и куратору ИБ. Выполняет полученные рекомендации и предписания от НКЦКИ. Проводит расследование КИ ЗОКИИ и информирует куратора ИБ и старшего диспетчера о результатах проведённого расследования.	Телефоны: - рабочий, - мобильный	xxx@mos.ru		Приказ (распоряжение) от XX.XX.XXXX № XXX
8.	ФИО, администратор	Эксплуатирует и администрирует ЗОКИИ. Участвует в мероприятиях по выявлению, реагированию и расследованию КИ ЗОКИИ.	Телефоны: - рабочий, - мобильный	xxx@mos.ru		Приказ (распоряжение) от XX.XX.XXXX № XXX

⁹ Действия проводятся в нерабочее время, выходные и праздничные дни.

Раздел 5. Условия привлечения подразделений и должностных лиц ФСБ России

Для каждого ЗОКЦИИ/ОКЦИИ могут быть добавлены и другие условия, при которых могут привлекаться подразделения и должностные лица ФСБ России.

Условиями привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА являются следующие:

КИ привёл к прекращению функционирования ЗОКЦИИ.

Выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ, связанного с функционированием ЗОКЦИИ (восстановить штатное функционирование ЗОКЦИИ).

В НКЦКИ направлено сообщение о КИ, связанном с функционированием ЗОКЦИИ с указанием в нем необходимости привлечения подразделений и должностных лиц ФСБ России и причин, по которым выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ.

Раздел 6. Порядок проведения мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА в отношении ЗОКЦИИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России

Доклад заместителя руководителя организации по вопросам ИБ (ФИО) руководству организации (ФИО) о необходимости привлечения подразделений и (или) должностных лиц ФСБ России к проведению мероприятий по реагированию на КИИ и принятию мер по ликвидации последствий КА.

Решение руководителя организации о необходимости привлечения подразделений и должностных лиц ФСБ России (получение согласования на привлечения курирующего ОИВ).

В течение 30 минут:

Внесение в карточку КИ отметки о привлечении должностных лиц ФСБ России к реагированию на КИ и ликвидации последствий КА (ФИО, должность).

Подготовка и направление в НКЦКИ дополнительных материалов (ФИО, должность).

Получение от НКЦКИ подтверждения о привлечении ФСБ России.

Заместитель руководителя организации по вопросам ИБ организует взаимодействие с подразделениями и должностными лицами ФСБ России.

Приложение 4
к Методическим рекомендациям

Рекомендуемый шаблон приказа о возложении обязанностей по реагированию на КИ и принятию мер по ликвидации последствий КА и об утверждении Плана реагирования на КИ и принятия мер по ликвидации последствий КА

№ _____

О возложении обязанностей по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак на значимом объекте критической информационной инфраструктуры «Наименование информационной системы» и об утверждении Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на значимом объекте критической информационной инфраструктуры «Наименование информационной системы»

В целях реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и приказа ФСБ России от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации», а так же в целях подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак на значимом объекте критической информационной инфраструктуры (далее – КИИ) «Наименование информационной системы», **приказываю:**

1. Возложить на _____ (ФИО, наименование должности) обязанности по принятию решений о реализации мероприятий Плана реагирования на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак на значимом объекте КИИ «Наименование

информационной системы» (далее – План), на время его отсутствия обязанности возлагаются на _____ (ФИО, наименование должности).

2. Возложить на _____ (ФИО, наименование должности) обязанности по предоставлению сведений о компьютерных инцидентах на ЗОКИИ «Наименование информационной системы» в Департамент информационных технологий города Москвы, Департамент здравоохранения города Москвы, в Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) и в Федеральную службу по надзору в сфере связи, информационных технологий и массовых, на время его отсутствия обязанности возлагаются на _____ (ФИО, наименование должности).

3. Возложить на _____ (ФИО, наименование должности) обязанности по организации взаимодействия с подразделениями и должностными лицами ФСБ России в рамках реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на значимом объекте КИИ «Наименование информационной системы», на время его отсутствия обязанности возлагаются на _____ (ФИО, наименование должности).

4. Возложить на _____ (ФИО, наименование должности) обязанности по определению очередности реагирования на компьютерные инциденты на отдельных сегментах значимого объекта КИИ «Наименование информационной системы», на время его отсутствия обязанности возлагаются на _____ (ФИО, наименование должности).

5. Утвердить План (приложение).

6. _____ (ФИО, наименование должности,) довести приказ до сведения ответственных лиц в части, касающейся.

7. _____ (ФИО, наименование должности,) направить копию Плана в НКЦКИ в срок не позднее 7 календарных дней со дня его утверждения.

8. Контроль за выполнением настоящего приказа оставляю за собой.

Должность _____

_____ (ФИО)

Приложение 5
к методическим рекомендациям

Рекомендуемая форма карточки КИ

Форма регистрации компьютерного инцидента №			
1. Тема сообщения			
2. Дата и время возникновения инцидента			
3. Контактные данные работника, обрабатывающего компьютерный инцидент			
ФИО		Адрес	
Организация		Подразделение/ должность	
Контактные данные		e-mail	
4. Общее описание компьютерного инцидента			
Технические параметры инцидента (состав технических параметров компьютерного инцидента)			
Наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой			
Описание выявленного инцидента (характер воздействия, описание объектов, вовлеченных в инцидент, источник воздействия, наличие лог- файлов, и другие сведения об инциденте)			
Время информирования ФСБ России о КИ в период проведения оценки защищенности			

Подпись _____

(ФИО, должность, дата и время)

Приложение 6

к Методическим рекомендациям

Рекомендуемая форма журнала учёта КИ

[illegible]

Приложение 7
к Методическим рекомендациям

Подход к определению уровней влияния компьютерных инцидентов

Критерии	Уровни влияния			
	Критический	Высокий	Средний	Низкий
Ущерб в социальной сфере	Ущерб здоровью 500 человек или более	Ущерб здоровью от 50 до 500 человек	Ущерб здоровью от 1 до 50 человек	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности
Ущерб в политической сфере	Прекращение или нарушение функционирования Администрации Президента РФ, Правительства РФ и т.п.	Прекращение или нарушение функционирования федерального органа государственной власти	Прекращение или нарушение функционирования органа государственной власти субъекта РФ или города федерального значения	
Экономический ущерб	Ущерб, выраженный в снижении уровня дохода по всем видам деятельности более чем на 20 % от годового объема доходов, усредненного за прошедший 5-летний период	Ущерб, выраженный в снижении уровня дохода по всем видам деятельности от 10 до 20 % от годового объема доходов, усредненного за прошедший 5-летний период	Ущерб, выраженный в снижении уровня дохода по всем видам деятельности от 10 до 20 % от годового объема доходов, усредненного за прошедший 5-летний период	Снижение уровня дохода, которое не попадает под критерии других уровней
Ущерб в экологической сфере	Вредные воздействия на 5 000 человек и более	Вредные воздействия на 1 000 - 5 000 человек	Вредные воздействия на 1 000 - 5 000 человек	Вредные воздействия на людей, не попадающие под критерии других уровней
Ущерб для обеспечения обороны страны, безопасности государства и правопорядка	Прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента РФ, Правительства РФ и т.п.	Прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти	Прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта РФ или города федерального значения	

Приложение 8
к настоящим Методическим рекомендациям

**Пример оформления дополнительного раздела Плана «Мероприятия, проводимые в ходе проведения ФСБ России
оценки защищенности ОКИИ, подключенного к сети «Интернет»**

№ п/п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последоват ельность	Результат	Примеча ние
1. Обнаружение и регистрация КИ								
1.1.	Незамедлительный доклад ответственного за ИБ участка о КИ	Устный доклад	Оператор АСУ	Ответственный за ИБ участка	Ч + 5 мин.			
1.2.	Незамедлительное информирование ответственного лица, уполномоченного предоставлять сведения о КИ в ФСБ России (заместителя руководителя организации по вопросам ИБ)	Устный доклад	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ	Ч + 10 мин.	После выполнения п. 1.1		
2. Определение вовлеченных в КИ элементов информационной инфраструктуры								
2.1.	Сбор сообщений от технических средств	СЗИ, серверов, активного сетевого оборудования и т.д.	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ	Ч + 15 мин.	После выполнения п. 1.2		
2.2.	Сбор сообщений от работников, пользователей,	Опрос / получение письменных объяснений	Ответственный за ИБ участка	Заместитель руководителя	Ч + 30 мин.	После выполнения п. 2.1		

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	привилегированных пользователей			организации по вопросам ИБ				
2.3.	Сбор доказательств	Журналы регистрации событий серверов, рабочих станций, сетевого активного оборудования, СЗИ, копий жестких дисков и других данных, собранных на предшествующих этапах и т.п.	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ	Ч + 45 мин.	После выполнения п 2.2		
2.4.	Сбор сведений об уязвимостях, посредством которых были реализованы угрозы ИБ	СЗИ, серверов, активного сетевого оборудования и т.д.	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ	Ч + 55 мин.	После выполнения п 2.3	Зафиксированное свидетельство	
2.5.	Определение очередности реагирования на КИ, исходя из оценки уровня влияния КИ и приоритета	Сбор информации по последствиям КИ, определение уровня влияния и приоритетов (по масштабу и по значимости вовлеченных СВТ	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ	Ч + 1 ч. 15 мин.	После выполнения п 2.4	Решение заместителя руководителя организации по вопросам ИБ об очередности реагирования на КИ	
3. Информирование УФСБ России по г. Москве и Московской области субъекту								
3.1.	Уведомление УФСБ России по г. Москве и	Электронная почта: moscow_mo@fsb.ru	Заместитель руководителя	Руководитель организации	Ч + 2 часа	После выполнения п. 2.5	Запись в карточке КИ о направлении	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	Московской области о нарушении функционирования ОКИИ		организации по вопросам ИБ				информации в ФСБ России	
4. Выявление последствий КИ								
4.1.	Выявление работоспособности СВТ	СЗИ, серверов, активного сетевого оборудования	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ	Ч + 3 ч. 30 мин.	После выполнения п. 3.1		
4.2.	Протоколирование выявленных последствий	АРМ	Оператор АСУ	Ответственный за ИБ участка	Ч + 3 ч. 40 мин.	Параллельно с п. 4.1	Внесение данных в протокол	
5. Ликвидация последствий КИ								
5.1.	Восстановление работоспособности ОКИИ (разворачивание резервных образов, восстановление данных из резервных копий, переход на резервное оборудование, обновление программного обеспечения и антивируса, проведение нагрузочного тестирования)	АРМ, резервные образы, резервные копии, резервное оборудование, обновление программного обеспечения и антивируса, проведение нагрузочного тестирования и т.д.	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ	Ч + 4 ч. 30 мин.	После выполнения п. 4.1		

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
5.2.	Протоколирование действий по ликвидации последствий КИ	АРМ	Оператор АСУ	Ответственный за ИБ участка	Ч + 4 ч. 40 мин.	Параллельно с п. 5.1	Внесение данных в протокол	
5.3.	Доклад о произведенных работах по ликвидации последствий КИ заместителю руководителя организации по вопросам ИБ	Личный доклад	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ	Ч + 5 ч. 30 мин.	После выполнения п. 5.2		
6. Закрытие КИ при проведении оценки защищенности								
6.1.	Направление в УФСБ России по г. Москве и Московской области информации о восстановлении системы или не восстановлении системы	Электронная почта: <u>moscow_mo@fsb.ru</u>	Заместитель руководителя организации по вопросам ИБ	Руководитель организации	Ч + 10 ч.	После выполнения п. 5.3		
6.2.	Анализ причин неспособности ОКИИ противостоять угрозам информационной безопасности	План, протокол КИ, АРМ	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ	Ч + 24 ч.	После выполнения п. 6.1		

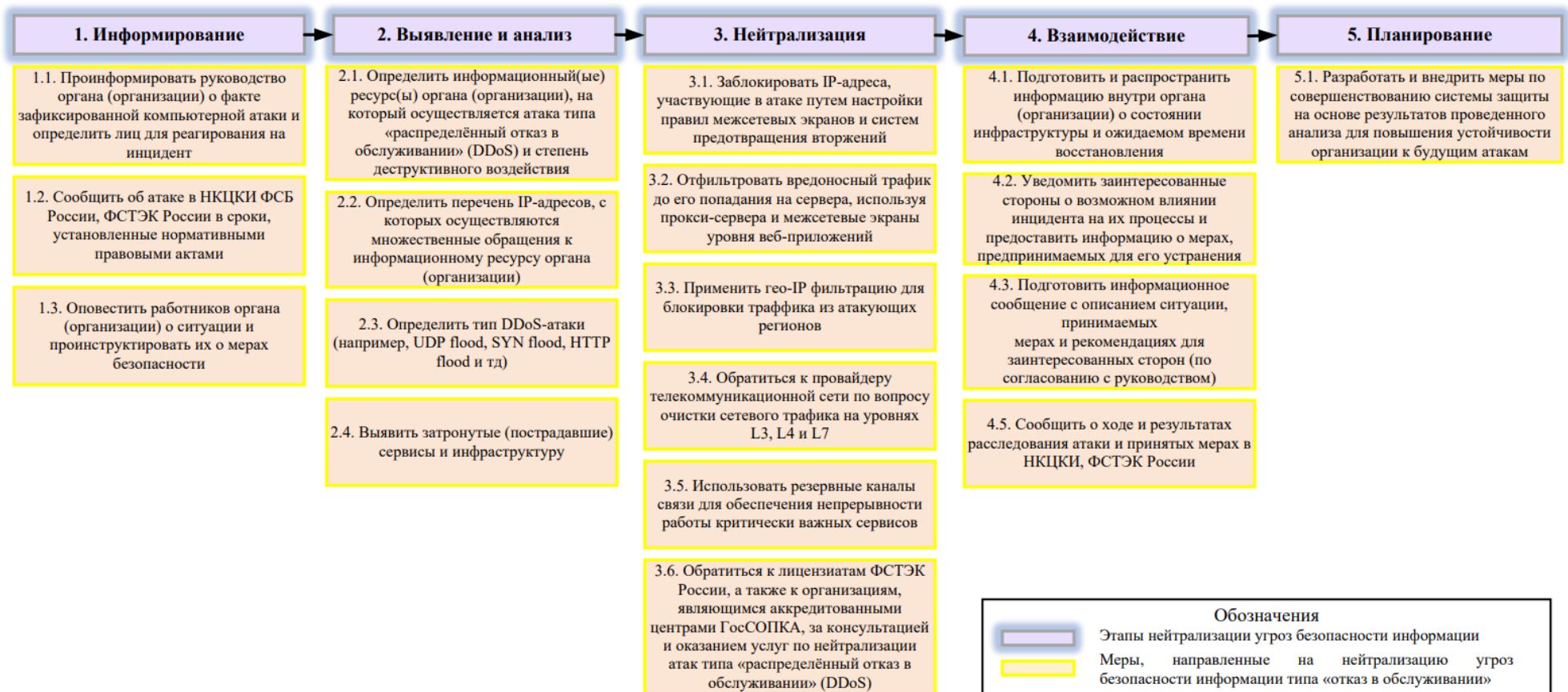
№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последоват ельность	Результат	Примеча ние
	в результате проведения оценки защищенности ФСБ России							
7. Внеочередная оценка показателя защищенности К_{зи}								
7.1.	Проведение внеочередной оценки показателя защищенности К _{зи}	Акты, протоколы, отчеты, внутренние организационно-распорядительные документы, эксплуатационная документация на СЗИ, результаты инвентаризации ИС, результаты опроса работников и т.д.	Ответственный за ИБ участка	Заместитель руководителя организации по вопросам ИБ				

Маркер (веха) этапа Плана	Временные отсечки (день-час-минута)								
	00-00-25	00-00-50	00-02-40	00-03-00	00-04-00	00-05-00	00-06-00	02-00-30	32-00-00
Этап 1. Обнаружение и регистрация КИ									
Дежурная бригада направлена на место размещения значимого объекта КИИ									
Этап 2. Определение вовлеченных в КИ элементов информационной инфраструктуры									
Решение заместителя руководителя субъекта КИИ об очередности реагирования на КИ по результатам определения оценки уровня влияния КИ и приоритета, внесение решения в протокол КИ									
Этап 3. Локализация КИ									
Решение куратора ИБ о локализации КИ, внесение решения в протокол КИ									
Этап 4. Информирование курирующего ОИВ, ДИТ, НКЦКИ, поставщиков услуг (подрядчиков) и внешних организаций									
Информация о подтверждении получения сведений о КИ курирующим ОИВ, ДИТ, поставщиками услуг, ЦОД доведена до руководства субъекта КИИ									
Этап 5. Выявление последствий КИ									

Маркер (веха) этапа Плана	Временные отсечки (день-час-минута)								
	00-00-25	00-00-50	00-02-40	00-03-00	00-04-00	00-05-00	00-06-00	02-00-30	32-00-00
Последствия КИ зафиксированы в протоколе									
Этап 6. Ликвидация последствий КИ									
Доклад старшему диспетчеру, куратору ИБ и заместителю руководителя организации по вопросам ИБ о восстановлении работоспособности значимого объекта КИИ или об отсутствии эффекта от проведенных мероприятий по восстановлению значимого объекта КИИ									
Этап 6.1. Привлечение ФСБ России к ликвидации последствий КИ (если работоспособность силами субъекта КИИ не восстановлена)									
Обеспечено взаимодействие с подразделениями и должностными лицами ФСБ России (Обеспечение прохода на территорию, предоставление должностным лицам ФСБ России, выделены АРМы, обеспечены точки входа для подключения к значимому объекту КИИ со служебного ноутбука									
Этап 7. Закрытие КИ									
В журнал КИ внесено время оповещения НКЦКИ о результатах расследования КИ									
Этап 8. Анализ результатов деятельности по управлению КИ									
В НКЦКИ направлена копия измененного Плана реагирования на КИ и принятия мер по ликвидации последствий КА									

Приложение 10
к настоящим методическим рекомендациям

Порядок действий обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в органах государственной власти и организациях при реализации угроз безопасности информации типа «отказ в обслуживании»

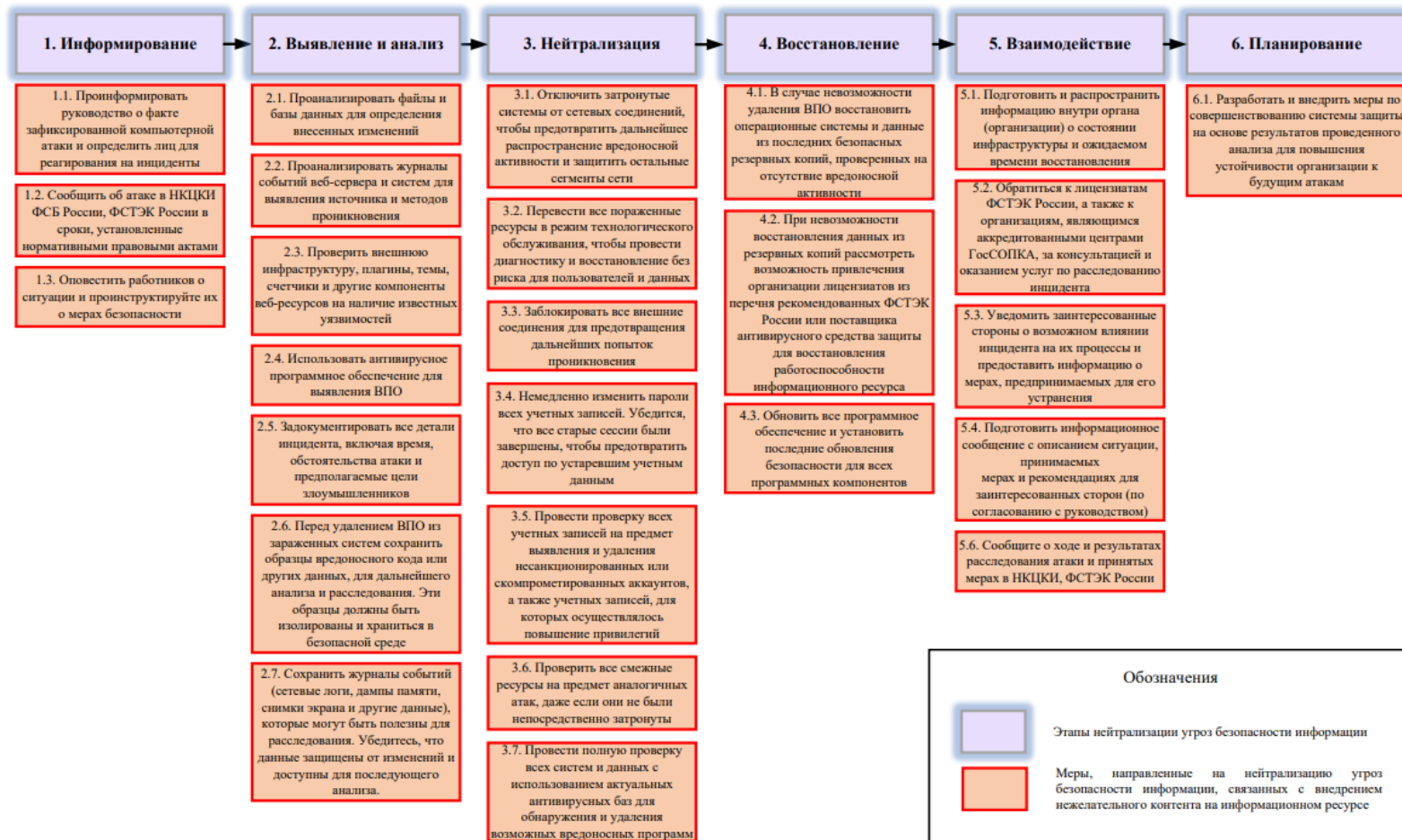


* Реализация указанного порядка не должна противоречить мероприятиям, предусмотренным Планом реагирования на компьютерные инциденты, разработка и реализация которых предусмотрена нормативными правовыми актами ФСБ России

Приложение 11

к настоящим методическим рекомендациям

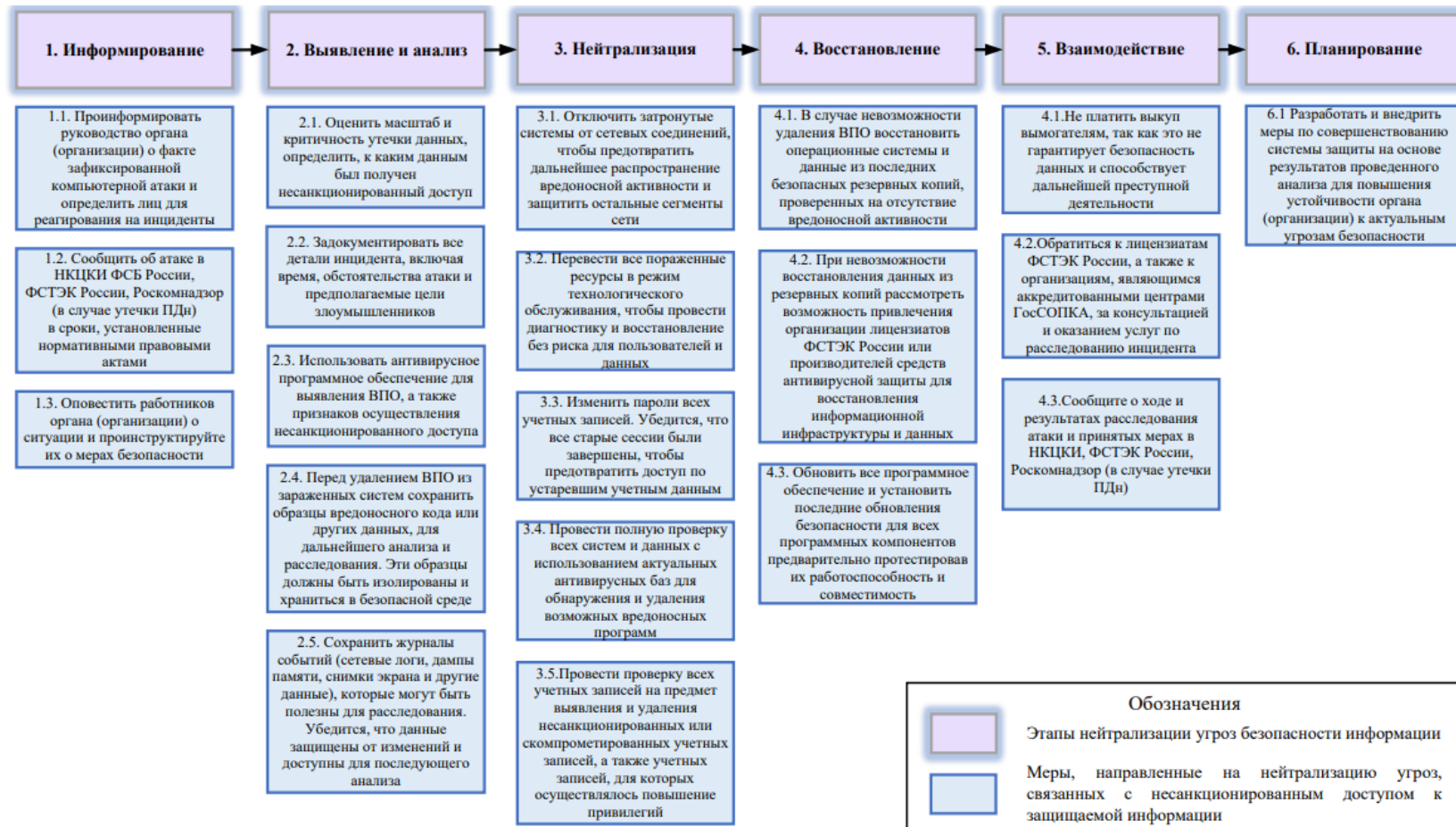
Порядок действий обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в органах государственной власти и организациях при реализации угроз безопасности информации, связанных с внедрением нежелательного контента на информационном ресурсе



* Реализация указанного порядка не должна противоречить мероприятиям, предусмотренным Планом реагирования на компьютерные инциденты, разработка и реализация которых предусмотрена нормативными правовыми актами ФСБ России

Приложение 12
к настоящим методическим рекомендациям

Порядок действий обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в органах государственной власти и организациях при реализации угроз безопасности информации, связанных с несанкционированным доступом к защищаемой информации

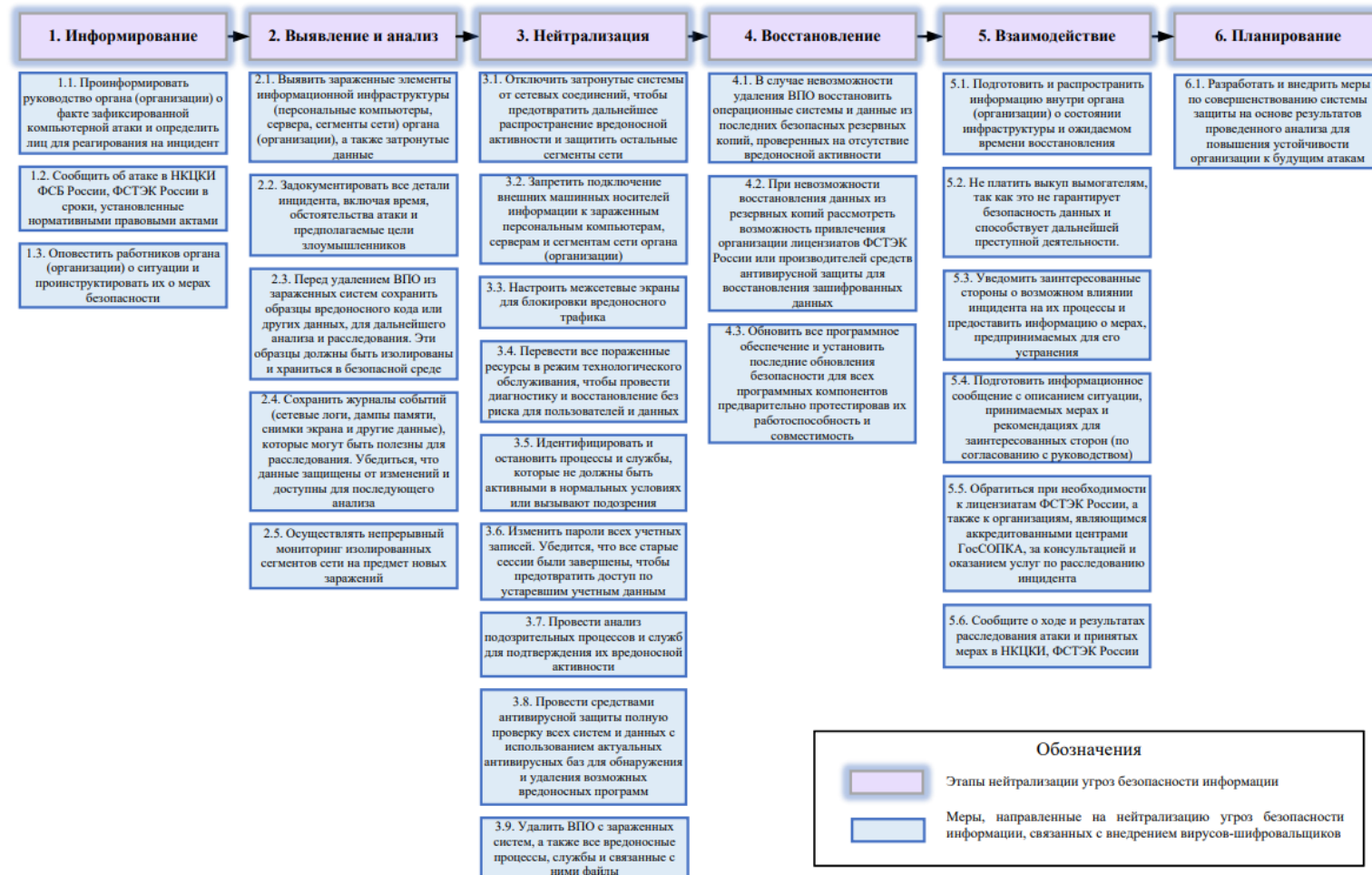


* Реализация указанного порядка не должна противоречить мероприятиям, предусмотренным Планом реагирования на компьютерные инциденты, разработка и реализация которых предусмотрена нормативными правовыми актами ФСБ России

Приложение 13

к настоящим методическим рекомендациям

Порядок действий обеспечению безопасности объектов критической информационной инфраструктуры и технической защиты информации в органах государственной власти и организациях при реализации угроз безопасности информации, связанных с внедрением вирусов-шифровальщиков



* Реализация указанного порядка не должна противоречить мероприятиям, предусмотренным Планом реагирования на компьютерные инциденты, разработка и реализация которых предусмотрена нормативными правовыми актами ФСБ России