



**НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ**

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО СОЗДАНИЮ  
ВЕДОМСТВЕННЫХ И КОРПОРАТИВНЫХ ЦЕНТРОВ  
ГОСУДАРСТВЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ  
И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА  
ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Москва, 2016

## Содержание

Термины и определения .....	4
1. Общие положения .....	9
1.1. Назначение документа.....	9
1.2. Корпоративные и ведомственные центры ГосСОПКА.....	10
1.3. Назначение и задачи центра ГосСОПКА .....	11
2. Принципы функционирования сегмента ГосСОПКА.....	13
2.1. Единство научно-технической политики .....	13
2.2. Кооперация сил и средств .....	14
2.3. Зона ответственности сегмента ГосСОПКА .....	16
2.4. Совершенствование деятельности по предупреждению, обнаружению и ликвидации последствий компьютерных атак.....	17
3. Функции сегмента ГосСОПКА и способы их реализации .....	19
3.1. Инвентаризация информационных ресурсов.....	19
3.2. Выявление уязвимостей информационных систем .....	21
3.3. Анализ угроз информационной безопасности .....	23
3.4. Повышение квалификации персонала информационных ресурсов .....	27
3.5. Прием сообщений о возможных инцидентах от персонала и пользователей информационных ресурсов .....	28
3.6. Обнаружение компьютерных атак .....	29
3.7. Анализ данных о событиях безопасности .....	30
3.8. Регистрация инцидентов .....	31
3.9. Реагирование на инциденты и ликвидация их последствий.....	33
3.10. Установление причин инцидентов.....	35
3.11. Анализ результатов устранения последствий инцидентов.....	36
4. Технические средства сегмента ГосСОПКА.....	39
5. Рекомендации по автоматизации технических средств сегмента ГосСОПКА.....	40
5.1. Автоматизация средств взаимодействия персонала.....	40
5.2. Автоматизация средств анализа событий безопасности.....	41
5.3. Автоматизация средств учета и обработки инцидентов .....	42
6. Рекомендации по обеспечению безопасности информации сегмента ГосСОПКА.....	44
7. Рекомендации по обеспечению деятельности сегмента ГосСОПКА .....	45
7.1. Рекомендации по организационной структуре .....	45
7.2. Рекомендации по организационно-методическому обеспечению.....	45
7.3. Рекомендации по кадровому обеспечению .....	47
7.4. Рекомендации по нормативному обеспечению .....	49
7.5. Рекомендации по финансовому обеспечению .....	50
8. Взаимодействие с НКЦКИ ГосСОПКА.....	51
8.1. Организация взаимодействия сегмента ГосСОПКА с НКЦКИ ГосСОПКА.....	51
8.2. Порядок обработки сообщений от НКЦКИ ГосСОПКА и сегмента ГосСОПКА.....	52

8.3. Порядок предоставления сведений в НКЦКИ ГосСОПКА .....	53
8.4. Перечень передаваемой информации о зоне ответственности сегмента ГосСОПКА.....	54
8.5. Перечень предоставляемой информации об информационных ресурсах .....	54
8.6. Перечень передаваемой информации о компьютерных атаках .....	55
8.7. Перечень предоставляемой информации о компьютерных инцидентах	56
8.8. Перечень предоставляемой информации о защищенности информационных ресурсов .....	63
8.9. Перечень предоставляемой информации о защищенности информационных ресурсов, доступных из сети Интернет .....	63
8.10. Перечень предоставляемой информации об угрозах информационной безопасности.....	64
8.11. Перечень возможных запросов НКЦКИ ГосСОПКА и порядок их обработки .....	64

## **Термины и определения**

1. Информационные ресурсы Российской Федерации — любая информация, зарегистрированная тем или иным образом на объекте информатизации (в информационной системе, в информационно-телекоммуникационной сети), находящемся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

2. Компьютерная атака — целенаправленное воздействие программными (программно-техническими) средствами на информационные системы, информационно-телекоммуникационные сети, средства связи и автоматизированные системы управления технологическими процессами, осуществляемое в целях нарушения (прекращения) их функционирования и (или) нарушения безопасности обрабатываемой ими информации.

3. Компьютерный инцидент — факт нарушения или прекращения функционирования объекта информационной инфраструктуры Российской Федерации и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе вызванный компьютерной атакой.

4. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) — единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак и федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

5. Субъект ГосСОПКА — федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Федерации, владельцы информационных ресурсов Российской Федерации, операторы связи, а также иные организации, осуществляющие лицензируемую деятельность в области защиты информации.

6. Зона ответственности субъекта ГосСОПКА — совокупность информационных ресурсов, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидация последствий компьютерных атак.

7. Силы обнаружения, предупреждения и ликвидации последствий компьютерных атак — подразделения субъектов ГосСОПКА и (или) специально выделенные сотрудники субъектов ГосСОПКА, на которых возложены обязанности проводить и участвовать в мероприятиях по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

8. Средства обнаружения, предупреждения и ликвидации последствий компьютерных атак — технологии, технические, программные, лингвистические, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

9. Обнаружение компьютерных атак — комплекс мероприятий по мониторингу и анализу функционирования информационных ресурсов с целью обнаружения компьютерных атак и компьютерных инцидентов.

10. Предупреждение компьютерных атак — комплекс превентивных мероприятий, направленных на снижение количества компьютерных инцидентов и повышение уровня защищенности информационных ресурсов.

11. Контроль (мониторинг) уровня (степени) защищенности информации (в информационной системе) — анализ и оценка функционирования системы защиты информации информационной системы,

изменения угроз безопасности информации, защищенности информации, содержащейся в информационной системе.

12. Ликвидация последствий компьютерных атак — комплекс мероприятий по восстановлению штатного режима функционирования информационных ресурсов после компьютерных инцидентов.

13. Уязвимость (информационного ресурса) — недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который может использоваться для реализации угроз безопасности обрабатываемой в ней информации.

14. Выявление уязвимостей — процесс выявления недостатков (включая уязвимости программного кода, ошибки в настройке, уязвимости архитектуры, ошибки в реализации мер защиты информации), которые могут использоваться нарушителем для проведения компьютерных атак.

15. Угроза (безопасности информации) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

16. Анализ угроз — процесс определения возможных способов реализации угроз безопасности информации, включая определение возможных способов проведения компьютерных атак на информационную систему с учетом особенностей реализованных в ней информационных технологий, а также состава ее технических средств и программного обеспечения.

17. Событие безопасности — идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

18. Корреляция событий ИБ — взаимосвязь двух или более событий безопасности.

19. Нормализация событий безопасности — приведение сообщений о событиях безопасности к единому формату.

20. Установление причин компьютерных инцидентов — комплекс взаимосвязанных и согласованных по целям, задачам, месту и времени, силам и средствам мероприятий, направленных на установление технических причин и условий возникновения компьютерных инцидентов, а также ликвидацию последствий данных инцидентов.

21. Анализ инцидента (первичный) — комплекс мероприятий по обработке информации о компьютерном инциденте, проводимых с целью выявления причин и источников возникновения инцидента, особенностей его реализации, нанесенного им ущерба, использованных уязвимостей, а также другой доступной входящей информации об инциденте.

22. Комплексный анализ инцидентов — исследование ряда выявленных компьютерных инцидентов с целью выявления закономерностей их возникновения и динамики распространения, классификации и типизации, разработки моделей развития, подготовки прогнозов угроз информационной безопасности и для прочих задач, связанных с повышением эффективности стратегий предупреждения, обнаружения и установления причин компьютерных инцидентов, реагирования на них и ликвидации их последствий.

23. Инвентаризация информационного ресурса — деятельность, направленная на сбор информации об информационном ресурсе, в том числе о соответствующих объектах информатизации, включая используемое в них аппаратное и программное обеспечение.

24. Тестирование на проникновение — метод контроля уровня защищенности, основанный на выявлении и анализе известных или ранее не известных уязвимостей, которые могут использоваться для получения несанкционированного доступа к информационному ресурсу.

25. Тестирование устойчивости к атакам «отказ в обслуживании» — метод контроля уровня защищенности информационного ресурса,

основанный на выявлении и анализе известных и ранее неизвестных уязвимостей, которые могут использоваться для нарушения доступности информационного ресурса.

26. Национальный координационный центр по реагированию на компьютерные инциденты (НКЦКИ) ГосСОПКА – наивысшая структура в иерархии ГосСОПКА, осуществляющая нормативное и методическое сопровождение ГосСОПКА.

27. Головной центр ГосСОПКА – наивысшая структура в иерархии центров, объединенных по ведомственному или организационному признакам.

28. Подчиненный центр ГосСОПКА – центр ГосСОПКА, имеющий структурное подчинение головному центру ГосСОПКА.

29. Центр ГосСОПКА – совокупность сил и средств субъекта ГосСОПКА, предназначенная для решения задач ГосСОПКА в своей зоне ответственности.

## **1. Общие положения**

### **1.1. Назначение документа**

1.1.1. Настоящие методические рекомендации описывают назначение, функции и принципы создания структурных элементов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее — ГосСОПКА) в части, касающейся деятельности ведомственных и корпоративных центров ГосСОПКА. Документ детализирует порядок создания центров ГосСОПКА, их функции, а также технические и организационные меры защиты информации, применяемые в ходе реализации этих функций.

1.1.2. Методические рекомендации разработаны в соответствии с основными положениями следующих нормативных документов:

Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

«Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 03.02.2012 № 803);

«Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (утв. Президентом РФ 12.12.2014 № К 1274).

1.1.3. Настоящий документ имеет рекомендательный характер и предназначен для:

органов государственной власти, принявших решение о создании ведомственных центров ГосСОПКА;

государственных корпораций, операторов связи и других организаций, осуществляющих лицензируемую деятельность в области защиты информации и принявших решение о создании корпоративных центров ГосСОПКА.

## **1.2. Корпоративные и ведомственные центры ГосСОПКА**

1.2.1. Основной организационно-технической составляющей ГосСОПКА являются центры ГосСОПКА, организованные по ведомственному и территориальному принципу, а также корпоративные центры ГосСОПКА.

1.2.2. Для охвата территориально распределенных информационных ресурсов могут создаваться структурные элементы более низкого уровня, организованные по территориальному принципу и подчиненные центрам ГосСОПКА (подчиненные центры ГосСОПКА).

1.2.3. Головной центр ГосСОПКА и иерархически подчиненные ему центры ГосСОПКА в совокупности образуют сегмент ГосСОПКА. Сегмент ГосСОПКА может быть образован единственным центром ГосСОПКА, в случаях отсутствия у него подчиненных центров. В этом случае центр ГосСОПКА образует сегмент ГосСОПКА.

1.2.4. Для решения задач ГосСОПКА заключается соглашение между НКЦКИ и головным центрами ГосСОПКА.

1.2.5. Ведомственные сегменты (центры) ГосСОПКА создаются органами государственной власти, а также организациями, осуществляющими лицензируемую деятельность в области защиты информации, действующими в интересах органов государственной власти.

1.2.6. Корпоративные сегменты (центры) ГосСОПКА создаются государственными корпорациями, операторами связи и иными организациями, осуществляющими лицензируемую деятельность в области защиты информации, в собственных интересах, а также для оказания услуг по предупреждению, обнаружению и ликвидации последствий компьютерных атак. Корпоративный сегмент ГосСОПКА может исполнять свои функции в

отношении информационных ресурсов органов государственной власти на основании договоров, заключаемых с владельцами указанных информационных ресурсов и (или) с операторами соответствующих государственных информационных систем.

### **1.3. Назначение и задачи центра ГосСОПКА**

1.3.1. Основным назначением головного центра ГосСОПКА и иерархически подчиненных ему центров является контроль за обеспечением защищенности информационных ресурсов, находящихся в зоне ответственности субъекта ГосСОПКА, от компьютерных атак, а также контроль за восстановлением штатного функционирования данных ресурсов при возникновении компьютерных инцидентов, вызванных компьютерными атаками.

1.3.2. К основным задачам центра ГосСОПКА относятся:

а) обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы;

б) проведение мероприятий по оценке степени защищенности контролируемых информационных ресурсов;

в) проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы;

г) сбор и анализ данных о состоянии информационной безопасности в контролируемых информационных ресурсах;

д) осуществление взаимодействия между центрами по вертикали иерархической структуры ГосСОПКА;

е) информирование в зоне ответственности субъекта ГосСОПКА заинтересованных лиц по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак;

ж) формирование и поддержание в актуальном состоянии информации о контролируемых информационных ресурсах.

1.3.3. Указанные выше задачи решаются путем выполнения центром ГосСОПКА и иерархически подчиненными ему центрами своих функций, определенных в разделе 3 настоящих методических рекомендаций. При этом:

а) головной центр ГосСОПКА выполняет свои функции в пределах всей зоны ответственности субъекта ГосСОПКА;

б) подчиненный центр ГосСОПКА выполняет свои функции в пределах выделенной ему зоны ответственности.

## **2. Принципы функционирования сегмента ГосСОПКА**

### **2.1. Единство научно-технической политики**

2.1.1. Деятельность всех структурных элементов сегмента ГосСОПКА подчиняется единой политике, устанавливаемой головным центром ГосСОПКА. При этом головной центр ГосСОПКА:

а) разрабатывает нормативные документы, определяющие порядок и особенности исполнения своих функций всеми структурными элементами сегмента ГосСОПКА;

б) определяет основные типы инцидентов, возможность возникновения которых поддается прогнозированию на основе имеющихся научно-технических возможностей сегмента ГосСОПКА (далее — типовые инциденты);

в) разрабатывает методические рекомендации по реализации комплекса мероприятий по обнаружению, предупреждению и ликвидации последствий типовых инцидентов, предназначенные для персонала сегмента ГосСОПКА и информационных ресурсов, находящихся в зоне его ответственности;

г) выполняет анализ результатов мероприятий по обнаружению, предупреждению и ликвидации последствий инцидентов и обеспечивает оценку их эффективности;

д) на основе анализа результатов указанных мероприятий уточняет (для типовых инцидентов) и разрабатывает (для инцидентов, не относившихся к типовым на момент возникновения) методические рекомендации по реализации комплекса мероприятий по обнаружению, предупреждению и ликвидации последствий инцидентов.

2.1.2. Сфера действия, условия, особенности и порядок применения методических рекомендаций, разработанных НКЦКИ ГосСОПКА, определяются:

а) для ведомственного сегмента ГосСОПКА — нормативными актами органа государственной власти, принявшего решение о создании сегмента ГосСОПКА;

б) для корпоративного сегмента ГосСОПКА — нормативными актами организации, принявшей решение о создании сегмента ГосСОПКА, и договорами, на основании которых производится включение информационных ресурсов в зону его ответственности.

## **2.2. Кооперация сил и средств**

2.2.1. Силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы включают в себя:

- а) персонал и технические средства сегмента ГосСОПКА;
- б) персонал и средства защиты, участвующие в реализации мер защиты информации информационных ресурсов, входящих в зону ответственности сегмента ГосСОПКА.

2.2.2. В отношении информационных ресурсов, находящихся в зоне ответственности сегмента ГосСОПКА, реализуются меры защиты информации, в том числе — обеспечивающие обнаружение, предупреждение и ликвидацию последствий компьютерных атак, в соответствии с требованиями, установленными законодательством Российской Федерации, иными нормативными актами, а также решениями владельцев информационных ресурсов. К мерам защиты информации, используемым при реализации ГосСОПКА относятся:

- а) анализ угроз безопасности информации и рисков их реализации;
- б) контроль (анализ) защищенности информации;
- в) управление конфигурацией средств защиты;
- г) регистрация и анализ событий безопасности;
- д) выявление инцидентов и реагирование на них;
- е) обеспечение действий в нештатных ситуациях;
- ж) информирование и обучение персонала.

2.2.3. Персонал и технические средства сегмента ГосСОПКА выполняют функции, определенные в разделе 3 настоящих методических рекомендаций.

2.2.4. При включении информационного ресурса в зону ответственности сегмента ГосСОПКА обеспечивается:

а) определение особенностей реализации мер защиты информации;  
б) контроль за реализацией указанных выше мер защиты информации;  
в) координация деятельности персонала при компьютерных инцидентах;  
г) оценка эффективности мер защиты информации, принимаемых для предупреждения и обнаружения компьютерных атак, а также действий по ликвидации их последствий;

д) нормативная и методическая помощь в совершенствовании мер защиты информации в части, относящейся к обнаружению, предупреждению и ликвидации последствий компьютерных атак;

е) взаимодействие средств защиты с техническими средствами сегмента ГосСОПКА.

2.2.5. Способы взаимодействия средств защиты информационных ресурсов, включаемых в зону ответственности сегмента ГосСОПКА, с техническими средствами сегмента ГосСОПКА и технические решения по их реализации разрабатываются в ходе работ по созданию сегмента ГосСОПКА.

2.2.6. При реализации мероприятий по кооперации сил и средств сегмент ГосСОПКА формирует рекомендации по реализации дополнительных мер защиты информации. Указанные рекомендации формируются на основе анализа угроз, актуальных для информационных ресурсов, находящихся в зоне ответственности сегмента ГосСОПКА.

2.2.7. Организация, принявшая решение о создании сегмента ГосСОПКА, может поручить выполнение отдельных функций, определенных в разделе 3 настоящих методических рекомендаций, организациям, осуществляющим лицензируемую деятельность в области защиты информации. Ответственность за выполнение таких функций несет сегмент ГосСОПКА.

### **2.3. Зона ответственности сегмента ГосСОПКА**

2.3.1. Деятельность сегмента ГосСОПКА осуществляется в соответствии с Конституцией и другими нормативными актами Российской Федерации. Зона ответственности сегмента ГосСОПКА определяется при принятии решения о его создании и может изменяться в процессе его функционирования.

2.3.2. Зоной ответственности ведомственных центров (сегментов) ГосСОПКА являются информационные ресурсы органов государственной власти, а также подчиненных им структурных подразделений и подведомственных организаций.

2.3.3. Зона ответственности корпоративного сегмента ГосСОПКА определяется организацией, создавшей сегмент ГосСОПКА, на основании решения руководителя организации, внутренних нормативных актов и заключенных договоров.

2.3.4. Включение информационных ресурсов в зону ответственности сегмента ГосСОПКА производится в процессе его функционирования на основании планов, учитывающих для каждого такого информационного ресурса возможные сроки проведения работ по организации взаимодействия средств защиты с техническими средствами сегмента ГосСОПКА, а также возможные сроки выполнения рекомендаций по усилению мер защиты информации, предъявляемых сегментом ГосСОПКА. Исключение информационных ресурсов из зоны ответственности сегмента ГосСОПКА не должно приводить к изменению полноты предоставляемых услуг по обнаружению, предупреждению и ликвидации последствий компьютерных атак для остальных участников ГосСОПКА.

2.3.5. При реализации мероприятий по включению и исключению из зоны ответственности сегмента ГосСОПКА информационных ресурсов органов государственной власти, государственных учреждений и корпораций Российской Федерации сегмент ГосСОПКА официально информирует об их

проведении федеральный орган исполнительной власти, уполномоченный в области создания и функционирования ГосСОПКА.

#### **2.4. Совершенствование деятельности по предупреждению, обнаружению и ликвидации последствий компьютерных атак**

2.4.1. Деятельность сегмента ГосСОПКА основана на постоянном накоплении опыта и совершенствовании методов предупреждения, обнаружения и ликвидации последствий компьютерных атак.

2.4.2. Методические документы, формируемые сегментом ГосСОПКА, и их перечень согласовываются с федеральным органом исполнительной власти, уполномоченным в области создания и функционирования ГосСОПКА.

2.4.3. При создании сегмента ГосСОПКА определяются основные типы компьютерных атак, предупреждение, обнаружение и ликвидация последствий которых обеспечиваются сегментом ГосСОПКА (далее — типовых компьютерных атак). Для указанных атак в ходе создания сегмента ГосСОПКА разрабатываются методические рекомендации, определяющие:

а) признаки, на основе которых производится обнаружение указанных атак и (или) регистрация инцидентов, связанных с их проведением (далее — индикаторы компрометации);

б) порядок действий персонала сегмента ГосСОПКА и информационных ресурсов, находящихся в зоне ответственности сегмента ГосСОПКА, при ликвидации последствий указанных атак.

2.4.4. При обнаружении и по итогам ликвидации последствий типовых компьютерных атак проводится оценка эффективности мер защиты информации, определяемых соответствующими методическими рекомендациями, и — при необходимости — доработка методов обнаружения и методических рекомендаций по их реализации.

2.4.5. По итогам ликвидации последствий инцидентов, вызванных компьютерными атаками, не относившихся к типовым на момент регистрации, проводится анализ способов проведения атаки, уязвимостей, использованных злоумышленником, а также, при необходимости, дополнительные

исследования. На основе полученных результатов данный вид компьютерных атак включается в число типовых и для него также разрабатываются методические рекомендации.

2.4.6. В ходе взаимодействия сегментов ГосСОПКА с НКЦКИ ГосСОПКА осуществляется обмен сведениями об инфраструктуре и компьютерных инцидентах, индикаторами компрометации и методическими рекомендациями по обнаружению, предупреждению и ликвидации последствий типовых компьютерных атак.

### **3. Функции сегмента ГосСОПКА и способы их реализации**

При создании сегмента ГосСОПКА реализуются следующие функции:

- инвентаризация информационных ресурсов;
- выявление уязвимостей информационных ресурсов;
- анализ угроз информационной безопасности;
- повышение квалификации персонала информационных ресурсов;
- прием сообщений о возможных инцидентах от персонала и пользователей информационных ресурсов;
- обеспечение процесса обнаружения компьютерных атак;
- анализ данных о событиях безопасности;
- регистрация инцидентов;
- реагирование на инциденты и ликвидация их последствий;
- установление причин инцидентов;
- анализ результатов устранения последствий инцидентов.

#### **3.1. Инвентаризация информационных ресурсов**

3.1.1. Целью инвентаризации является получение и поддержание в актуальном состоянии сведений об информационных ресурсах, необходимых для выполнения функций сегмента ГосСОПКА.

3.1.2. Деятельность по инвентаризации включает в себя следующие этапы сбора сведений об информационном ресурсе:

а) ФИО, должности и контактные данные лиц, ответственных за функционирование информационного ресурса;

б) доменные имена и сетевые адреса компонентов информационного ресурса (средств вычислительной техники, телекоммуникационного оборудования, виртуальных машин и т. п.) в соответствии с системой имен и сетевой адресацией информационного ресурса;

в) доменные имена и сетевые адреса компонентов информационного ресурса, доступные из сети Интернет, в соответствии с системой имен и сетевой адресацией сети Интернет, а также сведения о протоколах (включая

параметры транспортного уровня взаимодействия), по которым разрешен доступ к этим компонентам.

г) сведения о сегментации и топологии локальных вычислительных сетей, правилах маршрутизации и коммутации, настройках средств межсетевого экранирования;

д) перечень программного обеспечения (прикладного и системного), установленного на каждом средстве вычислительной техники;

е) параметры настройки программного и аппаратного обеспечения информационного ресурса, существенные с точки зрения обеспечения безопасности информации;

ж) параметры настройки средств обеспечения информационной безопасности.

3.1.3. Инвентаризацию информационных ресурсов рекомендуется проводить:

- не реже одного раза в квартал;
- для всех компонентов информационных ресурсов, находящихся в зоне ответственности сегмента ГосСОПКА (включая средства вычислительной техники, принадлежащие иным организациям, подключенные временно, предоставленные для тестирования и т. п.)
- при каждом изменении состава программного и (или) аппаратного обеспечения средств вычислительной техники, телекоммуникационного оборудования и виртуальных машин (путем ежедневного или событийного контроля изменений, а также иными способами, обеспечивающими уточнение инвентаризационной информации в течение одного рабочего дня с момента внесения изменений)

3.1.4. Сбор и уточнение инвентаризационной информации выполняются центром ГосСОПКА в пределах его зоны ответственности. Подчиненные центры ГосСОПКА предоставляют актуальную инвентаризационную информацию головному центру ГосСОПКА.

## **3.2. Выявление уязвимостей информационных систем**

3.2.1. Целью выявления уязвимостей является определение недостатков в обеспечении безопасности информационных ресурсов (включая уязвимости программного кода, ошибки в настройке, уязвимости архитектуры, ошибки в реализации мер защиты), которые могут использоваться нарушителем для проведения компьютерных атак. Выявление уязвимостей включает в себя оценку степени их опасности и разработку рекомендаций по их устранению. Результаты выявления уязвимостей должны соответствовать требованиям государственных стандартов ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» и ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».

3.2.2. Выявление уязвимостей производится для всех информационных ресурсов, входящих в зону ответственности сегмента ГосСОПКА. Выявление уязвимостей информационного ресурса проводится центром ГосСОПКА, в зоне ответственности которого находится информационный ресурс.

3.2.3. Выявление уязвимостей может выполняться следующими способами:

а) выявление известных уязвимостей сетевых служб, доступных для сетевого взаимодействия, с применением автоматизированных средств анализа защищенности (сетевое сканирование);

б) выявление известных уязвимостей программного обеспечения информационных ресурсов путем анализа состава установленного программного обеспечения и обновлений безопасности с применением автоматизированных средств анализа защищенности (системное сканирование, исследование с использованием привилегированных учетных записей и (или) программных агентов), а также других средств защиты информации;

в) тестирование на проникновение в условиях, соответствующих условиям нарушителя, действующего со стороны сети Интернет и (или) со

стороны информационных ресурсов, внешних по отношению к зоне ответственности сегмента ГосСОПКА;

г) тестирование на проникновение в условиях, соответствующих условиям нарушителя, действующего со стороны информационных ресурсов, входящих в зону ответственности сегмента ГосСОПКА;

д) тестирование устойчивости к атакам типа «отказ в обслуживании»;

е) контроль устранения ранее выявленных уязвимостей и недостатков;

ж) контроль выполнения требований безопасности информации, предъявляемых к контролируемой информационной системе;

з) анализ настроек программного и аппаратного обеспечения информационных систем, а также средств защиты информации;

и) анализ проектной, конструкторской и эксплуатационной документации информационных систем;

к) оценка соответствия применяемых мер защиты требованиям безопасности информации, предъявляемым к информационным ресурсам нормативными документами Российской Федерации и владельцев информационных ресурсов.

3.2.4. В случаях определенных нормативными документами Российской Федерации для выявления уязвимостей может применяться статический и динамический анализ исходного кода программного обеспечения информационных ресурсов (для программного обеспечения, поставляемого с исходными кодами).

3.2.5. Выявление уязвимостей рекомендуется проводить для каждого информационного ресурса со следующей периодичностью:

а) сетевое и системное сканирование, анализ настроек — не реже одного раза в месяц;

б) тестирование на проникновение и нагрузочное тестирование — не реже одного раза в год;

в) контроль выполнения требований безопасности информации — не реже одного раза в месяц;

г) контроль устранения ранее выявленных уязвимостей и недостатков — не реже одного раза в квартал;

д) оценка соответствия мер защиты — не реже одного раза в два года;

е) анализ проектной, конструкторской и эксплуатационной документации — перед вводом информационного ресурса в эксплуатацию и при каждом существенном изменении состава программных или аппаратных средств;

ж) анализ исходного кода — перед вводом информационного ресурса в эксплуатацию и при каждом изменении программного обеспечения, поставляемого с исходным кодом.

3.2.6. Подчиненные центры ГосСОПКА предоставляют актуальную информацию о выявленных уязвимостях головному центру ГосСОПКА путем отправки в головной центр ГосСОПКА отчетов с результатами всех проводимых мероприятий по данному направлению деятельности.

3.2.7. Центры ГосСОПКА обеспечивают хранение результатов выявления уязвимостей в течение трех лет с момента проведения соответствующих исследований. По запросу НКЦКИ ГосСОПКА предоставляются результаты выявления уязвимостей, проводившегося в отношении запрашиваемого информационного ресурса в заданный промежуток времени в пределах периода хранения результатов.

### **3.3. Анализ угроз информационной безопасности**

3.3.1. Целью анализа угроз информационной безопасности является определение возможных способов проведения компьютерных атак на информационную систему с учетом особенностей реализованных в ней информационных технологий, состава ее технических средств и программного обеспечения, а также разработка предложений по противодействию компьютерным атакам, представляющим угрозу соответствующим информационным ресурсам.

3.3.2. Анализ угроз проводится на основе инвентаризационной информации и результатов выявления уязвимостей и включает в себя:

а) определение возможных угроз, связанных с компьютерными атаками на данный информационный ресурс;

б) идентификацию уязвимостей, использование которых может позволить нарушителю выполнить такие атаки;

в) определение способов проведения компьютерных атак с использованием таких уязвимостей;

г) определение возможных признаков проведения таких компьютерных атак, способов их обнаружения и мер реагирования на них;

д) определение возможных путей противодействия проведению таких компьютерных атак;

е) выработку организационных и технических решений по противодействию компьютерным атакам.

3.3.3. Для каждой угрозы определяются возможные сценарии реализации, описываемые в терминах проведения компьютерной атаки или последовательности компьютерных атак, приводящих к достижению целей нарушителя. Описание компьютерной атаки включает в себя описания:

а) уязвимости или группы уязвимостей определенного типа, наличие которых делает возможным проведение атаки;

б) способа выполнения атаки с использованием данной уязвимости;

в) технических средств, необходимых для проведения атаки (по возможности, с примерами);

г) квалификации нарушителя, необходимой для проведения атаки;

д) возможных результатов атаки, способствующих достижению нарушителем своих целей;

е) возможных способов регистрации попытки проведения атаки.

3.3.4. На основе анализа угроз разрабатываются новые или уточняются существующие документы, включающие:

а) описания компьютерных атак, актуальных для информационных ресурсов, находящихся в зоне ответственности сегмента ГосСОПКА;

б) методические рекомендации по предупреждению, обнаружению и ликвидации последствий компьютерных атак;

в) решающие правила средств обнаружения компьютерных атак;

г) настройки средств обеспечения информационной безопасности;

д) политики обеспечения информационной безопасности;

е) нормативные правовые акты организации;

ж) дополнительные требования по обеспечению информационной безопасности для их включения в технические задания на создание новых, доработку и обслуживание существующих информационных ресурсов;

з) правила корреляции событий, направленные на определение попыток реализации угроз, связанных с проведением компьютерных атак;

и) инструкции для персонала информационных ресурсов по выявлению признаков проведения типовых компьютерных атак, порядку их обнаружения, действиям по ликвидации их последствий;

к) инструкции по действиям пользователей информационных ресурсов в случае возникновения инцидентов, связанных с компьютерными атаками;

л) требования к квалификации персонала и пользователей, необходимой для выполнения указанных выше инструкций.

3.3.5. Методические рекомендации по предупреждению, обнаружению и ликвидации последствий компьютерных атак являются общими для всех информационных ресурсов в зоне ответственности сегмента ГосСОПКА и должны включать в себя:

а) указания на основания и порядок принятия решения об инциденте, связанном с проведением компьютерной атаки (типового инцидента);

б) перечень и порядок принятия мер, направленных на предотвращение развития (локализацию) инцидента;

в) перечень и порядок сбора сведений, необходимых для установления причин инцидента;

г) перечень и описания возможных последствий инцидента;

д) перечень и порядок принятия мер, направленных на ликвидацию последствий инцидента;

е) описание порядка контроля мер локализации инцидента и ликвидации его последствий;

ж) перечень лиц, ответственных за принятие указанных выше мер, и (или) указание на порядок определения и назначения таких лиц.

#### 3.3.6. Головной центр ГосСОПКА:

а) разрабатывает рекомендации по уточнению общей модели угроз для различных классов информационных ресурсов, находящихся в зоне его ответственности, на основе обобщения сведений, полученных в результате инвентаризации и выявления уязвимостей;

б) разрабатывает методические рекомендации по предупреждению, обнаружению и ликвидации последствий компьютерных атак для сегмента ГосСОПКА;

в) оказывает методическую и экспертную поддержку подчиненным центрам ГосСОПКА;

г) проводит анализ информационных материалов, предоставляемых НКЦКИ ГосСОПКА, а также профильными информационными и новостными ресурсами, в которых описываются новые способы проведения компьютерных атак, новые типы уязвимостей и т. п.;

д) оценивает актуальность указанных проблем для информационных ресурсов, находящихся в зоне ответственности сегмента ГосСОПКА, прогнозирует возможность проведения новых типов атак и, исходя из этих прогнозов, планирует методическое обеспечение деятельности сегмента ГосСОПКА.

#### 3.3.7. Подчиненный центр ГосСОПКА:

а) определяет соответствие методических документов особенностям отдельных информационных ресурсов и по согласованию с головным центром уточняет методические рекомендации по предупреждению, обнаружению и

ликвидации последствий компьютерных атак для указанных информационных ресурсов;

б) совместно с персоналом информационных ресурсов разрабатывает инструкции для персонала по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

### **3.4. Повышение квалификации персонала информационных ресурсов**

3.4.1. С целью повышения квалификации персонала проводится обучение по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак. Повышение квалификации проводится:

а) путем ознакомления персонала с методическими рекомендациями и инструкциями по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак;

б) периодической оценки готовности персонала к действиям по обнаружению, предупреждению и ликвидации последствий компьютерных атак;

в) проведения дополнительного обучения персонала в соответствии с требованиями к квалификации персонала и недостатками, выявленными при оценке его готовности к действиям по обнаружению, предупреждению и ликвидации последствий компьютерных атак;

г) рассылки дополнительных информационных материалов по отдельным вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

3.4.2. Повышение квалификации персонала проводится владельцами информационных ресурсов самостоятельно, в рамках установленных трудовых отношений и в соответствии с внутренними нормативными документами. При этом центр ГосСОПКА разрабатывает рекомендации по программе обучения и выбору образовательных учреждений, обладающих необходимой компетенцией.

Подготовка и рассылка методических рекомендаций и информационных материалов по вопросам повышения квалификации осуществляются головным центром ГосСОПКА или делегируются подчиненным центрам ГосСОПКА.

3.4.3. Оценка готовности персонала к действиям при проведении нарушителями компьютерных атак проводится:

а) путем периодической аттестации персонала в соответствии с трудовым законодательством;

б) практической отработки действий персонала при имитации проведения компьютерных атак на информационные ресурсы.

### **3.5. Прием сообщений о возможных инцидентах от персонала и пользователей информационных ресурсов**

3.5.1. Центр ГосСОПКА обеспечивает централизованный прием сообщений о возможных компьютерных инцидентах с использованием средств взаимодействия с персоналом и пользователями информационных систем. Рекомендации по реализации средств взаимодействия приведены в разделе 5.1 настоящих методических рекомендаций.

3.5.2. Центр ГосСОПКА принимает сообщения, сформулированные в произвольной форме, в том числе — лицами, не обладающими необходимыми техническими знаниями. При наличии в сообщении неточностей, отсутствии необходимых сведений и т. п. и при возможности диалога с автором сообщения специалисты центра ГосСОПКА уточняют полученные сведения.

При приеме сообщений специалист центра ГосСОПКА определяет следующий состав сведений об инциденте:

а) контактную информацию лица, сообщившего о компьютерном инциденте (если автор сообщения согласен предоставить такую информацию);

б) наименование информационных ресурсов, вовлеченных в компьютерный инцидент, а при невозможности такой идентификации — любые сведения, позволяющие прямо или косвенно определить такие ресурсы;

- в) время обнаружения инцидента;
- г) характер инцидента, как его понимает и может сформулировать автор сообщения;
- д) сведения о принятых мерах, которыми располагает автор сообщения.

3.5.3. При получении сообщения специалист центра ГосСОПКА проводит регистрацию компьютерного инцидента в системе учета и обработки инцидентов путем создания карточки инцидента, в которую вносит все полученные сведения независимо от их полноты и достоверности.

### **3.6. Обнаружение компьютерных атак**

3.6.1. Целью обнаружения компьютерных атак является своевременное реагирование на связанные с ними инциденты, принятие мер по ликвидации последствий таких инцидентов.

3.6.2. В ходе деятельности по обнаружению компьютерных атак реализуются следующие процессы:

- а) контроля за реализацией единых правил эксплуатации средств обнаружения компьютерных атак на информационные ресурсы, находящиеся в зоне ответственности сегмента ГосСОПКА;

- б) контроля за централизованным обновлением баз решающих правил для средств обнаружения компьютерных атак сегмента ГосСОПКА;

- в) выявления ранее неизвестных компьютерных атак сетевого уровня, в том числе с применением средств анализа сетевого трафика на каналах связи;

- г) выявления ранее неизвестных компьютерных атак, проводимых с использованием вредоносного программного обеспечения, в том числе с использованием методов поведенческого анализа программного обеспечения;

- д) разработки решающих правил для неизвестных компьютерных атак.

3.6.3. При обнаружении ранее неизвестных компьютерных атак центром ГосСОПКА проводятся мероприятия по реализации функции анализа угроз информационной безопасности, представленные в разделе 3.3. настоящего документа.

### **3.7. Анализ данных о событиях безопасности**

3.7.1. Целью анализа данных о событиях безопасности является регистрации инцидентов, в том числе связанных с ранее неизвестными компьютерными атаками, а также инцидентов, связанных с недостаточной эффективностью принимаемых мер защиты информации. Обработка (сбор, анализ и хранение) данных о событиях безопасности производится центрами ГосСОПКА в зонах их ответственности. Рекомендации по реализации средств автоматизированного анализа данных о событиях безопасности приведены в разделе 5.2 настоящих рекомендаций.

3.7.2. Для реализации анализа данных центрами ГосСОПКА осуществляется сбор результатов работы всех средств защиты информации, используемых в соответствии с политикой безопасности, принятой в информационных системах, находящихся в зоне ответственности сегмента ГосСОПКА, в том числе:

а) средств обнаружения атак и межсетевых экранов, применяемых на каналах связи, по которым осуществляется доступ к информационным ресурсам;

б) средств анализа сетевого трафика, использующих методы интеллектуального анализа данных;

в) средств обнаружения атак и межсетевых экранов, применяемых в локальных вычислительных сетях, в которых размещены компоненты информационных ресурсов;

г) средств поведенческого анализа программного обеспечения;

д) средств регистрации событий операционных систем, прикладного программного обеспечения, телекоммуникационного оборудования.

3.7.3. Сбор информации из указанных источников рекомендуется проводить в автоматизированном режиме. При этом реализуются правила нормализации событий информационной безопасности.

3.7.4. Сведения о событиях безопасности сопоставляются со сведениями об уязвимостях компонентов информационных ресурсов для прогнозирования возможных действий злоумышленника при проведении компьютерных атак.

3.7.5. При проведении анализа данных о событиях безопасности с использованием автоматизированных средств применяются правила корреляции. При выполнении одного или нескольких правил корреляции, свидетельствующих о возможной попытке реализации угроз безопасности, определенных ранее в ходе анализа угроз, в системе учета и обработки инцидентов создается карточка инцидента.

3.7.6. Правила корреляции определяются сотрудниками центра ГосСОПКА с учетом сведений, полученных на этапах инвентаризации и выявления уязвимостей информационных ресурсов. В процессе функционирования сегмента ГосСОПКА проводится постоянная работа по адаптации источников данных о событиях безопасности со средствами их анализа для повышения эффективности обнаружения компьютерных атак, а также работа по формированию новых правил корреляции и сигнатур.

### **3.8. Регистрация инцидентов**

3.8.1. Регистрация инцидентов осуществляется с использованием автоматизированных средств учета и обработки инцидентов. Рекомендации по реализации учета и обработки инцидентов приведены в разделе 5.3 настоящих рекомендаций.

3.8.2. Карточка инцидента, созданная в центре ГосСОПКА, являющимся головным подразделением сегмента ГосСОПКА, на основе сообщения пользователя или в результате анализа данных о событиях безопасности, направляется в подчиненный центр ГосСОПКА, в зоне ответственности которого находится информационный ресурс, предположительно затрагиваемый инцидентом. В случае если инцидент затрагивает несколько информационных ресурсов, карточка инцидента направляется во все подчиненные центры ГосСОПКА, в зоне ответственности которых находятся указанные информационные ресурсы.

3.8.3. При получении карточки инцидента специалист центра ГосСОПКА проводит следующие мероприятия:

- а) проверяет и уточняет сведения о возможном инциденте;
- б) подтверждает факт возникновения инцидента и принимает решение о начале действий по реагированию на него;
- в) определяет первоочередные меры реагирования на инцидент, определяет ответственных лиц и направляет им задания на реагирование.

3.8.4. В ходе проверки и уточнения сведений о возможном инциденте специалист центра ГосСОПКА:

- а) направляет лицам, ответственным за функционирование информационных ресурсов, предположительно затрагиваемых инцидентом, запрос на проверку сведений, содержащихся в карточке инцидента;
- б) проводит самостоятельную проверку карточки инцидента путем сопоставления содержащихся в ней сведений с данными, полученными в процессе инвентаризации, выявления уязвимостей и анализа событий.

В случае если сведения о возможном инциденте подтверждаются специалистом центра ГосСОПКА или хотя бы одним из лиц, ответственных за функционирование хотя бы одного из информационных ресурсов, инцидент признается подтвержденным и принимаются меры реагирования.

3.8.5. По результатам проверки и уточнения карточка инцидента должна включать в себя как минимум следующие сведения:

- а) первичное сообщение об инциденте, если инцидент зарегистрирован на основании полученного сообщения, а также контактную информацию лица, сообщившего о инциденте, при ее наличии;
- б) наименования информационных систем, вовлеченных в компьютерный инцидент;
- в) состав технических средств информационного ресурса, вовлеченного в инцидент;
- г) время возникновения инцидента;
- д) тип зафиксированного воздействия;

- е) сведения о зафиксированных нарушениях штатного режима функционирования объектов информационного ресурса;
- ж) сведения о принятых персоналом информационного ресурса мерах;
- з) сведения о динамике развития инцидента с учетом принятых мер;
- и) сведения о расположении ресурса;
- к) дополнительные сведения об инциденте, которые могут быть полезны при реагировании на инцидент и ликвидации его последствий, при их наличии.

### **3.9. Реагирование на инциденты и ликвидация их последствий**

#### **3.9.1. Реагирование на инцидент включает в себя:**

- а) фиксацию состояния и анализ объектов информационных ресурсов, вовлеченных в инцидент;
- б) координацию деятельности по прекращению воздействия компьютерных атак, проведение которых вызвало возникновение инцидента;
- в) фиксацию и анализ сетевого трафика, циркулирующего в информационном ресурсе, вовлеченном в инцидент;
- г) определение причин инцидента и возможных его последствий для информационного ресурса;
- д) локализацию инцидента;
- е) сбор сведений для последующего установления причин инцидента;
- ж) планирование мер по ликвидации последствий инцидента;
- з) ликвидацию последствий инцидента;
- и) контроль ликвидации последствий;
- к) формирование рекомендаций для совершенствования нормативных документов, в соответствии с которыми осуществляется деятельность центра ГосСОПКА и специалистов, обеспечивающих информационную безопасность информационных ресурсов.

3.9.2. При отсутствии в центре ГосСОПКА специалистов, обладающих необходимой квалификацией, к реагированию на инцидент могут обоснованно привлекаться специалисты центра ГосСОПКА, стоящего выше в иерархии ГосСОПКА.

3.9.3. Определение причин инцидента проводится специалистом центра ГосСОПКА совместно с персоналом информационного ресурса. При этом:

а) специалист центра ГосСОПКА оперирует данными инвентаризации, выявления уязвимостей и анализа событий безопасности, а также направляет лицу, ответственному за функционирование информационного ресурса, запросы на предоставление дополнительных сведений;

б) персонал информационного ресурса действует в пределах своей компетенции в соответствии с инструкциями, а также в соответствии с указаниями специалиста центра ГосСОПКА.

3.9.4. В случае если запрос специалиста центра ГосСОПКА предполагает выполнение действий, не предусмотренных эксплуатационной документацией информационного ресурса и способных привести к нарушению его функционирования, решение о допустимости выполнения запроса принимает — с учетом обстоятельств инцидента — лицо, ответственное за функционирование информационного ресурса.

3.9.5. Лицо, ответственное за функционирование информационного ресурса, совместно со специалистами центра ГосСОПКА организует локализацию инцидента и ликвидацию последствий в соответствии методическими рекомендациями, разработанными для инцидентов данного типа.

3.9.6. Координация действий по реагированию на инцидент возлагается на специалиста центра ГосСОПКА. Специалист центра ГосСОПКА, формирует рабочую группу, состоящую из специалистов, ответственных за функционирование затронутых инцидентом информационных ресурсов. Рабочая группа принимает решение о мерах по локализации инцидента.

3.9.7. Решения принимаются рабочей группой отдельно для каждого информационного ресурса, затронутого инцидентом. Каждое решение утверждается лицом, ответственным за функционирование информационного ресурса, по согласованию со специалистом центра ГосСОПКА, координирующим действия по реагированию на инцидент. Решения,

затрагивающие функционирование прочих информационных ресурсов, принимаются по согласованию с лицами, ответственными за их функционирование.

Решения о ликвидации последствий инцидента принимаются в аналогичном порядке по результатам установления причин инцидента.

### **3.10. Установление причин инцидентов**

3.10.1. Установление причин инцидента проводится в две стадии.

- а) первичный анализ инцидента;
- б) комплексный анализ инцидента.

3.10.2. Задачами первичного анализа инцидента являются:

- а) установление обстоятельств и возможных последствий инцидента;
- б) своевременное установление обстоятельств инцидента, выходящих за рамки стандартного порядка действий при инциденте данного типа.

3.10.3. Задачами комплексного анализа инцидента являются:

- а) установление причин инцидента;
- б) установление фактических последствий инцидента.

3.10.4. Первичный анализ инцидента проводится одновременно с локализацией инцидента центром ГосСОПКА, в зоне ответственности которого находится информационный ресурс, в отношении которого возник инцидент. Комплексный анализ инцидента проводится одновременно с ликвидацией его последствий совместно с головным центром ГосСОПКА.

3.10.5. На обеих стадиях осуществляется сбор сведений об инциденте и их анализ. Сведениями об инциденте могут являться:

- а) следы действий нарушителя (данные, непосредственно свидетельствующие о действиях нарушителя, например, образцы программного кода или передававшиеся данные);
- б) данные регистрации событий;
- в) сведения (сообщения, объяснения) очевидцев и предоставленные ими объективные подтверждения (снимки экрана, тексты электронных сообщений, фрагменты записи сетевого трафика);

г) результаты измерений производительности вычислительных средств;  
д) результаты выполнения мероприятий по обнаружению компьютерных атак.

3.10.6. Сбор сведений по пунктам а) – г) раздела 3.10.5 осуществляется персоналом информационных ресурсов. В отдельных случаях (при отсутствии у персонала необходимой квалификации или подозрении о причастности персонала к инциденту) по согласованию с лицом, ответственным за функционирование информационного ресурса, к сбору сведений привлекаются специалисты центра ГосСОПКА, в зоне ответственности которого находится информационный ресурс.

3.10.7. В ходе анализа сведений делаются выводы об обстоятельствах инцидента, характере атаки, а также возможных путях развития инцидента и его последствиях. Сведения об инциденте сохраняются для последующей разработки или уточнения методических рекомендаций по обнаружению, предупреждению и ликвидации последствий аналогичных инцидентов. Сбор и анализ сведений проводятся на протяжении всего комплекса мероприятий по ликвидации последствий инцидента.

В случае необходимости рассматривается вопрос передачи информации об инциденте в правоохранительные органы для проведения расследования.

### **3.11. Анализ результатов устранения последствий инцидентов**

3.11.1. Инцидент признается завершенным после принятия всех мер, предусмотренных методическими рекомендациями и (или) решением рабочей группы, при условии, что установление причин инцидента показало достаточность принятых мер.

3.11.2. Анализ результатов устранения последствий инцидента включает в себя оценку:

а) вреда, причиненного информационному ресурсу и его владельцу в результате инцидента;

б) недостатков в обеспечении безопасности информации, не позволивших предотвратить инцидент;

- в) своевременности обнаружения инцидента;
- г) действий персонала при локализации инцидента и ликвидации его последствий;
- д) сроков устранения последствий инцидента.

3.11.3. При оценке вреда, причиненного информационному ресурсу и его владельцу в результате инцидента, принимаются в расчет:

- а) трудозатраты персонала и иные затраты, связанные с ликвидацией последствий;
- б) вред, причиненный общественным интересам и интересам владельца информационного ресурса, в том числе связанный с нарушением конфиденциальности, целостности и доступности сведений, обрабатываемых затронутыми информационными ресурсами.

3.11.4. При оценке недостатков в обеспечении безопасности информации определяются:

- а) нормативные требования, невыполнение, недостаточная эффективность выполнения или отсутствие которых сделали инцидент возможным;
- б) дополнительные меры защиты, которые не являются обязательными в соответствии с действующими нормативными документами, но которые могли бы предотвратить инцидент.

На основании оценки вреда и недостатков разрабатываются рекомендации по предупреждению подобных инцидентов и стандартный порядок действий при их повторении.

3.11.5. При оценке своевременности обнаружения инцидента принимаются в расчет:

- а) сведения об инциденте, выявленные в ходе установления его причин, на основании которых можно судить о времени фактического начала компьютерной атаки, которая привела к инциденту;
- б) время, прошедшее с фактического начала компьютерной атаки до регистрации инцидента.

Решение о своевременности обнаружения инцидента принимается лицами, ответственными за функционирование информационных ресурсов, затронутых инцидентом. В случае если обнаружение инцидента признается несвоевременным хотя бы для одного из затронутых информационных ресурсов, разрабатываются предложения по совершенствованию применяемых технических средств и процедур обнаружения, предупреждения и ликвидации последствий компьютерных атак.

3.11.6. При оценке действий персонала по локализации инцидента и ликвидации его последствий принимаются в расчет:

- а) сроки выполнения действий;
- б) достаточность квалификации персонала.

В случае если признается неудовлетворительной оценка локализации инцидента и ликвидации его последствий или признается недостаточной квалификация персонала информационного ресурса, затронутого инцидентом, разрабатываются предложения по совершенствованию порядка принятия решений и повышению квалификации персонала.

3.11.7. По результатам анализа инцидента, связанного с ранее неизвестной компьютерной атакой, центр ГосСОПКА осуществляет самостоятельную разработку или уточнение существующих методических рекомендаций по обнаружению, предупреждению и ликвидации последствий компьютерных атак данного типа.

В случае если разработка указанных рекомендаций вызывает затруднение, центр ГосСОПКА направляет запрос в НКЦКИ ГосСОПКА на оказание методической помощи по разработке указанных рекомендаций.

#### **4. Технические средства сегмента ГосСОПКА**

4.1. Функции сегмента ГосСОПКА могут быть выполнены с использованием следующих технических средств:

- а) средства взаимодействия персонала;
- б) средства взаимодействия с НКЦКИ ГосСОПКА;
- в) средства инвентаризации информационных систем;
- г) средства выявления уязвимостей;
- д) средства анализа событий безопасности;
- е) средства учета и обработки инцидентов.

При этом рекомендуется обеспечить интеграцию технических средств, указанных в пунктах в) – е).

4.2. Интеграция указанных технических средств должна обеспечивать:

а) передачу вышестоящему структурному подразделению сегмента ГосСОПКА информации, обрабатываемой соответствующим техническим средством;

б) консолидацию вышестоящим структурным элементом сведений, полученных от нижестоящих структурных элементов;

в) возможность привлечения специалистов вышестоящего структурного элемента к выполнению функций нижестоящего структурного элемента (в том числе — с предоставлением защищенного удаленного доступа к соответствующим техническим средствам).

## **5. Рекомендации по автоматизации технических средств сегмента ГосСОПКА**

Технические средства сегмента ГосСОПКА (средства взаимодействия с персоналом и пользователями информационных систем, анализа данных о событиях безопасности, регистрации инцидентов и реагирования на них) могут быть реализованы с использованием автоматизации.

### **5.1. Автоматизация средств взаимодействия персонала**

5.1.1. Взаимодействие персонала, эксплуатирующего информационные ресурсы и средства защиты, с персоналом сегмента ГосСОПКА может обеспечиваться с использованием:

а) существующих в организации или специально созданных в центре ГосСОПКА средств автоматизации взаимодействия;

б) телефонной связи.

5.1.2. Средства автоматизации взаимодействия являются основным средством, реализация которого должна обеспечивать следующие технологические процессы:

а) информирования о деятельности сегмента ГосСОПКА;

б) приема текстовых сообщений о возможных компьютерных инцидентах, связанных с информационными ресурсами, находящимися в зоне ответственности сегмента ГосСОПКА, от любых заинтересованных лиц (в том числе — анонимных);

в) двустороннего обмена электронными сообщениями между специалистами сегмента ГосСОПКА и зарегистрированными пользователями.

Дополнительные функциональные возможности средств автоматизации взаимодействия могут быть реализованы в ходе работ по созданию сегмента ГосСОПКА.

5.1.3. Телефонная связь является вспомогательным способом оперативного взаимодействия.

## **5.2. Автоматизация средств анализа событий безопасности**

5.2.1. В процессе автоматизированного анализа данных о событиях информационной безопасности могут выполняться следующие процессы:

- а) сбор сведений от различных источников данных о событиях безопасности;
- б) хранение сведений;
- в) нормализация собранных сведений;
- г) агрегация событий безопасности (определение соответствия данных, зарегистрированных разными источниками, одному и тому же событию безопасности);
- д) определение причинно-следственных связей между событиями на основе правил корреляции;
- е) каскадирование событий (учет событий, зарегистрированных на основе применения правил корреляции, при анализе прочих, в том числе ранее обработанных, событий);
- ж) регистрация событий безопасности на основе анализа причинно-следственных связей;
- з) автоматическое формирование оповещения об обнаружении компьютерной атаки;
- и) прогнозирование возможного развития атаки.

5.2.2. В зависимости от возможностей и инфраструктуры центра ГосСОПКА часть указанных процессов может выполняться персоналом центра ГосСОПКА.

5.2.3. Оповещение об обнаружении компьютерной атаки должно содержать сведения:

- а) о типе проводимой атаки;
- б) времени ее регистрации;
- в) источнике и объекте атаки.

5.2.4. Прогнозирование возможного развития атаки может осуществляться путем отображения:

а) компонентов информационных ресурсов, которые станут доступны нарушителю для взаимодействия в случае, если в результате атаки он получит несанкционированный доступ к объекту атаки;

б) компонентов информационных ресурсов, потенциально подверженных аналогичной атаке.

5.2.5. В процессе анализа данных пользователь средств автоматизированного анализа может запрашивать следующую информацию:

а) инвентаризационные данные заданного компонента информационного ресурса;

б) сведения об уязвимостях заданного компонента информационного ресурса;

в) сведения об исходных и нормализованных событиях безопасности, относящихся к информационному ресурсу в целом и его заданному компоненту.

5.2.6. Средства анализа данных о событиях информационной безопасности должны обеспечивать масштабирование.

5.2.7. При адаптации средств анализа данных к новым типам компьютерных атак могут выполняться следующие процессы:

а) редактирование существующих правил корреляции;

б) разработка и тестирование собственных правил корреляции.

### **5.3. Автоматизация средств учета и обработки инцидентов**

5.3.1. Средства учета и обработки инцидентов должны обеспечивать регистрацию инцидентов путем создания заявок на их обработку (карточек компьютерных инцидентов). Создание карточек инцидентов может проводиться вручную специалистом сегмента ГосСОПКА (при получении сообщений) или автоматически на основании результатов работы средств анализа событий безопасности.

5.3.2. В процессе учета и обработки инцидентов могут использоваться следующие операции с карточкой инцидента:

а) ввод и редактирование сведений, относящихся к инциденту;

б) прикрепление к карточке инцидента дополнительных сведений в виде файлов произвольного формата;

в) изменение статуса инцидента;

г) управление доступом к карточке инцидента;

д) регистрация действий, выполняемых с карточкой инцидента;

е) поиск карточек инцидентов по заданным критериям.

5.3.3. При работе с карточкой инцидента в нее могут быть включены следующие сведения:

а) дата и время создания карточки инцидента;

б) идентификатор лица, создавшего карточку инцидента;

в) описание инцидента;

г) идентификаторы информационных ресурсов, затронутых инцидентом;

д) инвентаризационная информация об информационных ресурсах, затронутых инцидентом;

е) рекомендации по ликвидации последствий инцидента;

ж) протокол решений, принимаемых в ходе ликвидаций последствий инцидента, и действий, предпринимаемых на основании этих решений;

з) результаты анализа инцидента;

и) дополнительные сведения (включая информацию, использованную в ходе установления причин инцидента) в виде файлов произвольного формата, прикрепляемых к карточке инцидента.

## **6. Рекомендации по обеспечению безопасности информации сегмента ГосСОПКА**

6.1. Безопасность информации, обрабатываемой техническими средствами сегмента ГосСОПКА, обеспечивается персоналом сегмента ГосСОПКА на всех стадиях (этапах) ее создания и в ходе эксплуатации.

6.2. Безопасность информации обеспечивается путем принятия организационных и технических (программно-технических) мер по защите информации в рамках системы защиты информации сегмента ГосСОПКА.

6.3. Система и средства защиты информации сегмента ГосСОПКА, а также программно-технические средства автоматизации взаимодействия должны соответствовать требованиям действующего законодательства Российской Федерации.

## **7. Рекомендации по обеспечению деятельности сегмента ГосСОПКА**

### **7.1. Рекомендации по организационной структуре**

7.1.1. Сегмент ГосСОПКА создается на основе существующих структурных подразделений организации, выполняющих функции, связанные с обеспечением безопасности информационных ресурсов. При необходимости должно быть обеспечено целевое выделение дополнительных штатных ресурсов (подразделений, специалистов), а также подготовка, переподготовка и повышение квалификации кадров.

7.1.2. Ведомственный центр ГосСОПКА создается на основе подразделений федерального уровня территориально-административной структуры ведомства. Допускается создание ведомственного центра ГосСОПКА на основе иных подразделений, в том числе — в структуре организации ведомственного подчинения, при условии, что действующие нормативные документы ведомства наделяют данное структурное подразделения полномочиями, необходимыми для осуществления деятельности по защите информации в интересах всего ведомства.

Обособленные ведомственные центры ГосСОПКА при необходимости создаются в территориальных подразделениях ведомства уровня федерального округа или субъекта федерации, а также в организациях ведомственного подчинения.

7.1.3. Центр ГосСОПКА корпоративного сегмента создается с учетом организационной и территориальной структуры организации, принявшей решение о создании сегмента ГосСОПКА.

### **7.2. Рекомендации по организационно-методическому обеспечению**

7.2.1. Организационно-методическое обеспечение сегмента ГосСОПКА устанавливает принципы и основные положения, регламентирующие деятельность по обнаружению, предупреждению и ликвидации последствий компьютерных атак.

7.2.2. Организационно-методическое обеспечение представляет собой набор организационно-распорядительных документов, разработанных

центром ГосСОПКА в виде политик, регламентов, инструкций и т. п. и утвержденных руководством организации, принявшей решение о создании сегмента ГосСОПКА.

Положения, установленные организационно-методическим обеспечением, должны быть доведены до всех специалистов сегмента ГосСОПКА.

7.2.3. Основные положения организационно-методического обеспечения должны определять:

а) требования, выполнение которых необходимо для осуществления своевременного обнаружения, предупреждения и ликвидации последствий компьютерных атак;

б) меры, обеспечивающие предотвращение и (или) снижение негативного влияния инцидентов на функционирование информационных ресурсов, находящихся в зоне ответственности сегмента ГосСОПКА;

в) порядок координации деятельности работников структурных подразделений сегмента ГосСОПКА в рамках процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак;

г) порядок взаимодействия с НКЦКИ ГосСОПКА;

д) политику и регламенты выполнения структурными элементами сегмента ГосСОПКА их функций.

7.2.4. Рекомендуется рассматривать следующие стадии обнаружения компьютерных атак и реагирования на них:

а) стадия обнаружения, оповещения и оценки, на которой путем анализа события информационной безопасности и установленных критериев выявляется инцидент, производятся оповещение уполномоченных сотрудников, оценка инцидента, принятие решений о дальнейшем реагировании на инцидент;

б) стадия сбора и фиксации информации, относящейся к инциденту;

в) стадия закрытия инцидента, включающая локализацию (предотвращение распространения) инцидента и восстановление штатного функционирования информационного ресурса;

г) стадия анализа собранной информации, относящейся к инциденту, и принятия управленческих решений по результатам реагирования на инцидент.

### **7.3. Рекомендации по кадровому обеспечению**

7.3.1. В штатном расписании подразделений, на которые возложено выполнение функций центра ГосСОПКА выделяются три категории специалистов:

а) специалисты первой линии выполняют функции, связанные с взаимодействием сегмента ГосСОПКА с персоналом и пользователями информационных ресурсов и с НКЦКИ ГосСОПКА, а также функции, связанные с анализом событий безопасности и обеспечением функционирования технических средств сегмента ГосСОПКА;

б) специалисты второй линии выполняют функции, связанные с проведением инвентаризации информационных ресурсов, выявлением уязвимостей и анализом угроз, реагированием на компьютерные инциденты и ликвидацией их последствий, повышением квалификации пользователей и персонала информационных систем, а также эксплуатацией дополнительных средств защиты;

в) специалисты третьей линии выполняют функции, связанные с экспертной поддержкой специалистов первой и второй линий, анализом причин компьютерных инцидентов, оценки защищенности, разработкой нормативных и методических документов, связанных с деятельностью сегмента ГосСОПКА.

7.3.2. Специалистам центра ГосСОПКА назначаются роли в соответствии с выполняемыми ими функциями. Рекомендуемый перечень ролей и соответствующих им функций приведен в таблице 1.

Таблица 1. Роли специалистов сегмента ГосСОПКА

Роль	Функции
<b>Специалисты первой линии</b>	
Специалист по взаимодействию с персоналом и пользователями	Прием сообщений персонала информационных ресурсов, взаимодействие с НКЦКИ ГосСОПКА
Специалист по обнаружению компьютерных атак и инцидентов	Анализ событий безопасности, регистрация инцидентов
Специалист по обслуживанию технических средств сегмента ГосСОПКА	Обеспечение функционирования технических средств, размещаемых в центре ГосСОПКА, а также дополнительных средств защиты информационных систем
<b>Специалисты второй линии</b>	
Специалист по оценке защищенности	Проведение инвентаризации информационных ресурсов, анализ выявленных уязвимостей и угроз, установление соответствия требований по информационной безопасности принимаемым мерам
Специалист по ликвидации последствий компьютерных инцидентов	Координация действий при реагировании на компьютерные атаки
Специалист по установлению причин компьютерных инцидентов	Установление причин инцидентов, анализ последствий инцидентов
<b>Специалисты третьей линии</b>	
Аналитик-методист	Анализ информации, предоставляемой специалистами первой и второй линий; разработка нормативных документов и методических рекомендаций по выполнению функций сегмента ГосСОПКА; разработка рекомендаций по доработке нормативных и методических документов по вопросам информационной безопасности
Технический эксперт	Экспертная поддержка в соответствии со специализацией (вредоносное программное обеспечение, настройка средств защиты, применение специализированных технических средств, оценка защищенности и т. п.)
Юрист	Нормативно-правовое сопровождение деятельности сегмента ГосСОПКА

Роль	Функции
Руководитель	Управление деятельностью сегмента ГосСОПКА

7.3.3. Деятельность центра ГосСОПКА может обеспечиваться:

а) путем назначения соответствующих ролей работникам структурных подразделений организации;

б) путем заключения договоров на выполнение сторонними организациями, осуществляющими лицензируемую деятельность в области защиты информации, соответствующих функций центра ГосСОПКА.

7.3.4. В случае, когда отдельные функции сегмента ГосСОПКА выполняются путем привлечения сторонних организаций, допускается не включать в соответствующие штатные расписания специалистов с соответствующими ролями (за исключением руководителей). Количество специалистов, необходимых для выполнения каждой из ролей, определяется в ходе работ по созданию соответствующих структурных элементов сегмента ГосСОПКА на основании критериев и нормативов, установленных в организации, создающей сегмент. При заключении со сторонними организациями договоров на выполнение отдельных функций сегмента ГосСОПКА соответствующие требования к кадровому обеспечению данных функций предъявляются к исполнителю.

7.3.5. Руководители центра ГосСОПКА назначаются из числа работников соответствующих структурных подразделений организации, принявшей решение о создании сегмента ГосСОПКА. Для замещения руководителей на период трудовых отпусков, временной нетрудоспособности и в иных случаях назначаются постоянные заместители или лица, временно исполняющие обязанности руководителей, из числа работников соответствующих структурных подразделений организации.

#### **7.4. Рекомендации по нормативному обеспечению**

7.4.1. Нормативное обеспечение деятельности совершенствуется в течение всего времени функционирования сегмента ГосСОПКА. Локальные

нормативные акты, регулирующие деятельность сегмента ГосСОПКА, создаются:

- а) в ходе работ по созданию сегмента ГосСОПКА;
- б) в ходе функционирования сегмента ГосСОПКА на основе накопленного опыта реагирования на компьютерные инциденты, методических рекомендаций федерального органа исполнительной власти, уполномоченного в области создания и обеспечения функционирования ГосСОПКА, результатов научно-исследовательских работ.

7.4.2. Минимальный комплект нормативной документации сегмента ГосСОПКА, необходимый для заключения соглашения о взаимодействии с ГосСОПКА, должен включать:

- а) положение о сегменте ГосСОПКА;
- б) штатное расписание сегмента ГосСОПКА;
- в) должностные инструкции специалистов сегмента ГосСОПКА.

## **7.5. Рекомендации по финансовому обеспечению**

7.5.1. Финансирование ведомственного сегмента ГосСОПКА производится за счет бюджетных средств ведомства. При этом обеспечивается финансирование мероприятий по продлению лицензий на необходимое программное обеспечение ведомственного сегмента ГосСОПКА и заключению соответствующих лицензионных договоров.

7.5.2. Создание и модернизация элементов ведомственного сегмента ГосСОПКА может осуществляться силами ведомства при их наличии или в соответствии с проектно-сметной документацией, разрабатываемой в ходе опытно-конструкторских и проектных работ по созданию и (или) модернизации ведомственного сегмента ГосСОПКА.

## **8. Взаимодействие с НКЦКИ ГосСОПКА**

### **8.1. Организация взаимодействия сегмента ГосСОПКА с НКЦКИ ГосСОПКА**

8.1.1. Взаимодействие сегмента ГосСОПКА и НКЦКИ ГосСОПКА осуществляется на основании соглашения о взаимодействии и регламента взаимодействия. В данных документах определяются головные подразделения, выполняющие функции по взаимодействию, их обязанности, а также уточняются каналы связи и используемые криптографические средства защиты информации.

8.1.2. Головной центр ГосСОПКА является основным субъектом в сегменте ГосСОПКА по взаимодействию с НКЦКИ ГосСОПКА.

8.1.3. Центр ГосСОПКА взаимодействует с НКЦКИ ГосСОПКА посредством:

- а) постоянного канала связи через сеть Интернет;
- б) телефонной связи;
- в) периодического документооборота через почту (фельдъегерскую службу).

8.1.4. В рамках обмена через сеть Интернет поддерживаются следующие способы взаимодействия:

- а) обмен информацией через специализированные системы, такие как портал, или автоматизированный обмен данными автоматизированных подсистем и компонентов ГосСОПКА;
- б) обмен информацией и получение доступа к справочной информации с использованием средств автоматизации взаимодействия;
- в) переписка по электронной почте.

8.1.5. Специализированные системы обмена информации должны обеспечивать возможность взаимодействия как в ручном режиме (действия оператора), так и в автоматизированном (посредством API).

8.1.6. Все взаимодействие по сети Интернет осуществляется с использованием криптографических средств защиты информации, имеющих

сертификаты ФСБ России. В рамках взаимодействия центра ГосСОПКА и НКЦКИ ГосСОПКА посредством сети Интернет не допускается передача сведений, составляющих государственную тайну.

8.1.7. Взаимодействие по телефонной связи используется:

- а) для экстренных обращений и уведомлений;
- б) в случаях, когда взаимодействие через сеть Интернет невозможно, в том числе в результате инцидентов ИБ.

8.1.8. Центр ГосСОПКА должен предусмотреть учет информации, направленной в НКЦКИ ГосСОПКА посредством сети Интернет. Факт получения информации подтверждается уведомлением от НКЦКИ ГосСОПКА о получении информации с уникальным идентификатором полученной информации.

8.1.9. На этапе создания центра ГосСОПКА необходимо произвести согласование параметров функций центра ГосСОПКА в части форматов и протоколов взаимодействия с НКЦКИ ГосСОПКА.

## **8.2. Порядок обработки сообщений от НКЦКИ ГосСОПКА и сегмента ГосСОПКА**

8.2.1. НКЦКИ ГосСОПКА направляет, а сегмент ГосСОПКА принимает и обрабатывает следующие типы информационных сообщений:

- а) сведения об актуальных угрозах;
- б) сведения об актуальных уязвимостях;
- в) сведения о признаках компьютерных инцидентов на объектах в зоне деятельности сегмента ГосСОПКА;
- г) сведения об индикаторах компрометации информационных ресурсов;
- д) изменения и дополнения к методическим рекомендациям;
- е) запросы на предоставление дополнительной информации по компьютерным инцидентам и другим событиям ИБ.

8.2.2. НКЦКИ ГосСОПКА должен иметь возможность направить запрос на предоставление детальной информации о защищенности информационных

ресурсов, конкретном инциденте, признаке компьютерного инцидента или компьютерной атаке, а сегмент ГосСОПКА предоставить ответ на запрос.

8.2.3. Сегмент ГосСОПКА направляет, а НКЦКИ ГосСОПКА принимает и обрабатывает следующие типы информационных сообщений:

- а) информацию о зоне ответственности сегмента ГосСОПКА, включая результаты инвентаризации;
- б) данные о компьютерных атаках;
- в) данные о компьютерных инцидентах;
- г) общую информацию о защищенности информационных ресурсов;
- д) детальную информацию о защищенности информационных ресурсов, доступных из сети Интернет;
- е) статистические данные об актуальных для сегмента ГосСОПКА угрозах;
- ж) сведения о самостоятельно обнаруженных индикаторах компрометации информационных ресурсов.

### **8.3. Порядок предоставления сведений в НКЦКИ ГосСОПКА**

Взаимодействие осуществляется:

- а) инициативно — иницилирующая сторона направляет информацию (сообщение, справочную и иную информацию);
- б) по запросу (ответ на запрос) — в рамках запрошенного объема и установленных сроков;
- в) без регламентации — при доступе к базам знаний и portalу, системам, предполагающим возможность удаленного доступа, по мере необходимости;
- г) в соответствии с планом предоставления информации (ежедневно, еженедельно, ежемесячно, ежеквартально, ежегодно или с иной периодичностью);
- д) автоматизированно — для сопряженных систем постоянного обмена фактической и статистической информацией об угрозах и состоянии ИБ контролируемых объектов.

#### **8.4. Перечень передаваемой информации о зоне ответственности сегмента ГосСОПКА**

Сегмент ГосСОПКА поддерживает в актуальном состоянии и передает в НКЦКИ ГосСОПКА при изменении информацию о зоне ответственности, а именно:

- а) перечень информационных ресурсов;
- б) перечень используемых средств защиты, в том числе компонентов ГосСОПКА;
- в) перечень ресурсов, маршрутизируемых в сети Интернет;
- г) перечень доменных имен;
- д) территориальную привязку информационных ресурсов;
- е) сведения о подключении информационных ресурсов к другим объектам информационной инфраструктуры;
- ж) наименование провайдера, оказывающего услуги связи;
- з) перечень организаций, осуществляющих разработку, эксплуатацию, поддержку и (или) администрирование информационных ресурсов (название организации, ИНН, КПП, юридический адрес, контакты ответственных лиц).

#### **8.5. Перечень предоставляемой информации об информационных ресурсах**

В рамках взаимодействия по вопросам предоставления информации об информационных ресурсах центр ГосСОПКА предоставляет следующую информацию:

- а) перечень уникальных средств вычислительной техники (включая любое сетевое оборудование, например ИБП, сетевые МФУ, оборудование IP-телефонии);
- б) перечень уникальных моделей телекоммуникационного оборудования с указанием количества;
- в) перечень уникального используемого общесистемного программного обеспечения с указанием количества и версий;

г) перечень уникального используемого прикладного программного обеспечения с указанием количества и версий;

д) среднее время, необходимое для обновления общесистемного программного обеспечения при обнаружении в нем критически опасной уязвимости после получения обновления;

е) среднее время, необходимое для обновления прикладного программного обеспечения при обнаружении в нем критически опасной уязвимости после доработки ПО разработчиком;

ж) перечень уникальных средств защиты, установленных на рабочих станциях пользователей;

з) перечень уникальных средств защиты, установленных на серверном оборудовании;

и) перечень сопряженных сетей;

к) перечень АСУ ТП (при их наличии);

л) правила парольной политики, принятые в организации;

м) правила проведения инвентаризации;

н) модель угроз и модель нарушителя (злоумышленника);

о) правила установки обновлений.

## **8.6. Перечень передаваемой информации о компьютерных атаках**

8.6.1. В рамках взаимодействия по вопросам обмена информацией о компьютерных атаках передается следующая информация:

а) дата и время начала компьютерной атаки;

б) дата и время окончания компьютерной атаки;

в) IP-адреса источников компьютерных атак;

г) географическое расположение источника компьютерных атак (страна, город);

д) тип компьютерной атаки (перебор паролей, сканирование портов, сканирование директорий веб-приложений, фишинг, распространение ВПО, деятельность бот-сети, рассылка спама, эксплуатация уязвимостей, DDoS-атака и т. п.);

- е) способ выявления компьютерной атаки;
- ж) название информационного ресурса, на который направлена компьютерная атака;
- з) IP-адрес и (или) доменное имя узла, на который направлена компьютерная атака;
- и) описание компьютерной атаки (перечень полей описания совпадает с перечнем полей в соответствующем типе компьютерного инцидента);
- к) принятые меры.

8.6.2. События информационной безопасности, информирующие о компьютерной атаке, должны быть агрегированы по IP-адресу источника компьютерной атаки, IP-адресу и (или) доменному имени информационного ресурса, на который направлена компьютерная атака, и типу компьютерной атаки.

8.6.3. При передаче информации о компьютерной атаке центр ГосСОПКА должен обеспечить хранение трафика, в котором была обнаружена компьютерная атака, а также всех событий информационной безопасности средств защиты и средств ГосСОПКА на срок не менее 6 (шести) месяцев.

Сведения о компьютерных атаках передаются в НКЦКИ ГосСОПКА еженедельно.

## **8.7. Перечень предоставляемой информации о компьютерных инцидентах**

Для взаимодействия по вопросам обмена информацией о компьютерных инцидентах (КИ) используется следующая карточка компьютерного инцидента.

Общие поля:

1. Идентификатор инцидента (порядковый номер инцидента). Поле заполняется уникальным буквенно-числовым значением длиной не более 15 символов. Установленный формат идентификатора компьютерного инцидента не может быть изменен с течением времени.

2. TLP. Поле предназначено для маркировки конфиденциальной информации с целью указания аудитории ее дальнейшего распространения. Заполняется исходя из степени конфиденциальности передаваемой информации. Используются маркировки следующего типа:

**Red (Красный).** Ознакомление с информацией должно быть ограничено исключительно лицом, указанным в качестве адресата. Ознакомление с материалами с данной пометкой также возможно для руководителей участвующих сторон обмена и специалистов, в чьи полномочия входит решение вопросов соответствующей тематики сообщения. Без права передачи третьим лицам и сторонним организациям.

**Amber (Желтый).** Ознакомление с информацией должно быть ограничено кругом специалистов участвующих сторон, работников защищаемого информационного ресурса, сотрудников правоохранительных органов и специалистов сторонних организаций, привлекаемых к обеспечению защиты информации данного информационного ресурса. При передаче такой информации указанным лицам в сопроводительном тексте для них делается запись о недопустимости распространения направляемых сведений.

**Green (Зеленый).** Информация может быть передана для возможного ознакомления специалистам в сфере информационной безопасности и другим лицам. При распространении такой информации должно быть сохранено авторство первоисточника.

3. Статус инцидента. Возможны следующие статусы:

- меры приняты, инцидент исчерпан (вес — 0);
- меры приняты, инцидент не исчерпан (вес — 10).

Поле предназначено для указания состояния КИ. КИ является исчерпанным в случае, если вредоносные воздействия завершились и были приняты меры по предотвращению последствий компьютерного инцидента.

4. Необходимость содействия. Значение поля может быть:

- необходимо содействие (вес — 10);

- нет необходимости в содействии (вес — 0).

Какой именно тип содействия необходим, указывается в поле комментария в карточке КИ. НКЦКИ ГосСОПКА может оказывать следующие типы содействия:

- передача информации об IP-адресах и доменных именах, осуществляющих вредоносные воздействия, уполномоченным организациям в различных странах мира для принятия мер по предотвращению вредоносной деятельности на ресурсы Российской Федерации;

- прекращение вредоносной активности IP-адресов и доменных имен, находящихся в адресном пространстве Российской Федерации;

- получение дополнительной информации об участниках КИ из специализированных источников и баз знаний НКЦКИ ГосСОПКА;

- анализ образцов вредоносного программного обеспечения для последующего выявления управляющих серверов и анализа его жизненного цикла;

- анализ журналов, образов ОС и другой информации, полученной в рамках реагирования на компьютерные инциденты, с целью получения полной информации о КИ;

- анализ КИ на связи с другими инцидентами;

- консультации по предотвращению последствий КИ;

- координация деятельности заинтересованных сторон по ликвидации КИ и предотвращению их последствий;

- мероприятия по оценке защищенности.

5. Тип инцидента (один инцидент может иметь комбинированный тип):

Группа 1 (вес — 4):

- ВПО (включая АРТ и бот-агент);

- несанкционированный доступ;

- эксплуатация уязвимости;

Группа 2 (вес — 3):

- DoS/DDoS;
- перебор паролей;
- ЦУ бот-сети;

Группа 3 (вес — 2):

- фишинг (мошенничество);
- вредоносный ресурс;
- запрещенный контент (нарушение прав);

Группа 4 (вес — 1):

- сканирование ресурсов;
- спам;
- нарушение политики безопасности;
- другое (вес — 0).

6. Опасность инцидента:

Рассчитывается по формуле: вес статуса + вес содействия + вес типа инцидента.

7. Дата и время фиксирования инцидента (UTC+0).

8. Дата и время создания карточки инцидента (UTC+0).

9. Источник поступления информации об инциденте (если возможно указать; департамент, управление, отдел, средства, которыми был выявлен инцидент и т. п.).

10. Описание инцидента и комментарии (включая хронологию принятых мер).

11. Связь с другими инцидентами (по номеру идентификатора).

12. Контакты:

- контактное лицо, ответственное по данному инциденту (ФИО, номер МГТС, электронная почта);
- контакты пострадавшей стороны (если имеются);
- контакты возможного злоумышленника (если имеются);
- контакты технического специалиста на объекте (если имеются).

13. Описание полей карточки инцидента, специфичной по типу инцидента (набор полей может изменяться в зависимости от ситуации, подтипа инцидента или полноты известной информации по инциденту).

А. DoS/DDos:

- IP-адрес пострадавшей стороны;
- IP-адреса атакующих;
- тип атаки (если возможно определить);
- мощность атаки (если возможно определить; пакетов в секунду, байтов в секунду).

Б. Перебор паролей:

- IP-адрес пострадавшей стороны;
- IP-адреса атакующих;
- тип протокола;
- мощность атаки (если возможно определить; пакетов в секунду, байтов в секунду).

В. Сканирование ресурсов:

- IP-адрес пострадавшей стороны;
- IP-адрес атакующего;
- список сканируемых портов;
- методы сканирования или ПО (если возможно определить).

Г. Спам:

- IP-адрес пострадавшей стороны;
- IP-адреса атакующих;
- количество почтовых сообщений (если возможно определить).

Д. Фишинг (мошенничество):

- IP-адрес пострадавшей стороны;
- IP-адрес (URL) вредоносного ресурса;
- IP-адрес (URL) легитимного ресурса;
- ПО, используемое в мошеннических целях;

– адреса электронных ящиков, с которых поступило письмо с вложением;

- образец ВПО (если возможно получить);
- тип ВПО, хеш, идентификатор ВПО (если возможно определить);
- исходный код электронного письма или EML.

Е. Вредоносный ресурс:

- тип вредоносного ресурса (если возможно определить);
- IP-адрес пострадавшей стороны;
- IP-адрес (URL) вредоносного ресурса;
- тип ВПО, хеш, идентификатор ВПО с указанием лаборатории (при обнаружении, если возможно определить);

- образец ВПО (если возможно получить);
- эксплуатируемая CVE.

Ж. ВПО:

- IP-адрес бот-агента;
- тип и общие сведения о бот-сети (если возможно определить);
- ЦУ, доменное имя и IP-адрес (если возможно определить);
- тип ВПО, хеш, идентификатор ВПО (если возможно определить);
- образец ВПО (если возможно получить).

З. ЦУ бот-сети:

- IP-адрес и доменное имя ЦУ;
- тип и общие сведения о бот-сети;
- способ выявления.

И. Эксплуатация уязвимостей:

- задействованные IP-адреса;
- класс уязвимости;
- последствия эксплуатации уязвимости.

К. Несанкционированный доступ:

- IP-адрес пострадавшей стороны;

- IP-адрес атакующего;
- способ получения НСД, протокол (если возможно определить);
- последствия несанкционированного доступа.

Л. Запрещенный контент:

- IP-адрес и доменное имя пострадавшей стороны;
- IP-адрес атакующего;
- тип контента;
- что привело к размещению контента.

М. Нарушение политики безопасности (полное описание инцидента и вся дополнительная информация).

Н. Другое (полное описание инцидента и вся дополнительная информация).

При передаче информации о компьютерном инциденте в автоматическом режиме карточка инцидента передается в формате JSON или XML. Формат согласуется на этапе организации взаимодействия с каждым сегментом ГосСОПКА индивидуально.

Центр ГосСОПКА обеспечивает хранение всех событий безопасности, журналов прикладного программного обеспечения и другой информации, полученных в рамках компьютерного инцидента на срок не менее 6 (шести) месяцев.

Вне очереди направляются инциденты:

- с запросом содействия;
- по которым были приняты меры, но инцидент не исчерпан;
- инциденты группы 1 и группы 2.

Остальные компьютерные инциденты направляются при их локализации (статус: меры приняты, инцидент исчерпан).

## **8.8. Перечень предоставляемой информации о защищенности информационных ресурсов**

В рамках взаимодействия по вопросам предоставления информации о защищенности информационных ресурсов центр ГосСОПКА предоставляет следующую информацию:

- а) перечень выявленных за отчетный период уникальных уязвимостей информационных ресурсов и рейтинг их присутствия;
- б) перечень выявленных за отчетный период уникальных угроз информационных ресурсов и рейтинг их присутствия;
- в) результаты контроля устранения ранее выявленных уязвимостей;
- г) результаты тестирования на проникновение;
- д) результаты нагрузочного тестирования;
- е) перечень принятых мер по нейтрализации выявленных уязвимостей и недостатков.

На основании данной информации формируются уведомления об угрозах информационной безопасности.

## **8.9. Перечень предоставляемой информации о защищенности информационных ресурсов, доступных из сети Интернет**

В рамках взаимодействия по вопросам предоставления информации о защищенности информационных ресурсов, доступных из сети Интернет, центр ГосСОПКА предоставляет следующую информацию для каждого узла:

- а) IP-адрес узла;
- б) доменное имя, используем в сети Интернет, если определено;
- в) установленное общесистемное и прикладное программное обеспечение (с указанием версий и установленных обновлений);
- г) назначение и роль узла в сети Интернет;
- д) запущенные сетевые сервисы и соответствующие им порты и протоколы;
- е) правила межсетевого экранирования.

На основании данной информации формируются уведомления об угрозах информационной безопасности.

#### **8.10. Перечень предоставляемой информации об угрозах информационной безопасности**

В рамках взаимодействия между НКЦКИ ГосСОПКА и центром ГосСОПКА возможен обмен информацией об актуальных угрозах информационной безопасности с предоставлением следующей информации:

- а) тип угрозы;
- б) источник получения информации об угрозе;
- в) направленность угрозы информационной безопасности;
- г) описание угрозы информационной безопасности;
- д) время получения информации об угрозе информационной безопасности;
- е) запрос на оказание помощи и (или) выполнение мероприятий по нейтрализации угроз информационной безопасности.

#### **8.11. Перечень возможных запросов НКЦКИ ГосСОПКА и порядок их обработки**

НКЦКИ ГосСОПКА в адрес сегмента ГосСОПКА может направить запросы следующего типа:

- а) запрос актуализации сведений о зоне ответственности;
- б) запрос актуализации сведений об оценке защищенности;
- в) запрос мониторинга определенных событий информационной безопасности;
- г) запрос дополнительной информации о компьютерном инциденте, компьютерной атаке;
- д) запрос на выполнение действий сегментом ГосСОПКА.

При получении запроса сегмент ГосСОПКА информирует о его получении, присваивает уникальный идентификатор, назначает ответственное за его выполнение лицо и сообщает ориентировочные сроки выполнения запроса.