ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59709— 2022

Защита информации

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Термины и определения

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным казенным учреждением «Войсковая часть 43753» (в/ч 43753), Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2022 г. № 1375-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2022

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
Алфавитный указатель терминов 8
Приложение А (справочное) Классификационные схемы понятий предметной области «Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирования на компьютерные инциденты» 11
Библиография 15

Введение

В настоящем стандарте стандартизованы термины в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты для их дальнейшего использования при разработке национальных стандартов, нормативных правовых актов и методических документов.

Установленные в настоящем стандарте термины расположены в систематизированном порядке, отражающем систему понятий в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Для каждого понятия установлен один стандартизованный термин.

Заключенная в круглые скобки часть термина может быть опущена при использовании термина в документах по стандартизации.

Приведенные определения можно, при необходимости, изменять, вводя в них производные признаки, раскрывая значения используемых в них терминов, указывая объекты, входящие в объем определяемого понятия. Изменения не должны нарушать объем и содержание понятий, определенных в настоящем стандарте.

Стандартизированные термины набраны полужирным шрифтом, а их краткие формы, представленные аббревиатурой, — светлым.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ

Термины и определения

Information protection. Computer incident management. Terms and definitions

Дата введения — 2023—02—01

1 Область применения

Настоящий стандарт содержит термины и определения основных понятий, используемых в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, применяемых в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Термины, установленные в настоящем стандарте, предназначены для применения во всех видах документации, входящей в область применения стандарта.

Настоящий стандарт необходимо применять совместно с ГОСТ Р 27.102, ГОСТ Р 59547.

Термины, приведенные в настоящем стандарте, соответствуют положениям [1].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 27.102 Надежность в технике. Надежность объекта. Термины и определения

ГОСТ Р 59547 Защита информации. Мониторинг информационной безопасности. Общие положения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети «Интернет» или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

1 **государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;** ГосСОПКА: Единый

Издание официальное

территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Силы государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

2 **силы государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;** силы ГосСОПКА: Национальный координационный центр по компьютерным инцидентам (НКЦКИ), центры ГосСОПКА, а также подразделения и должностные лица субъектов ГосСОПКА, которые осуществляют деятельность в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

3 **субъекты государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;** субъекты ГосСОПКА: Государственные органы Российской Федерации, российские юридические лица и индивидуальные предприниматели, в силу закона или на основании заключенных соглашений, а также регламентов взаимодействия осуществляющие обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты.

Примечание — Порядок заключения соглашений и регламентов взаимодействия определяют документы уполномоченного федерального органа исполнительной власти.

4 **национальный координационный центр по компьютерным инцидентам;** НКЦКИ: Организация, осуществляющая на национальном уровне координацию деятельности сил субъектов ГосСОПКА по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, а также обмен информацией о компьютерных инцидентах с уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

5 **зона ответственности (субъекта ГосСОПКА):** Совокупность информационных ресурсов, в отношении которых субъект ГосСОПКА обеспечивает обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

6 **центр государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;** центр ГосСОПКА: Форма организации сил и средств ГосСОПКА по ведомственному, корпоративному, отраслевому и (или) территориальному принципам.

7 **специалист по взаимодействию с персоналом и пользователями (центра ГосСОПКА):** Сотрудник центра ГосСОПКА, осуществляющий прием сообщений от персонала и пользователей информационных ресурсов и подготовку информации для предоставления в НКЦКИ.

8 **специалист по обнаружению компьютерных атак и инцидентов (центра ГосСОПКА):** Сотрудник центра ГосСОПКА, осуществляющий анализ событий информационной безопасности (ИБ) с целью обнаружения компьютерных атак и инцидентов, а также регистрацию компьютерных атак и инцидентов.

9 **специалист по обслуживанию средств центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;** специалист по обслуживанию средств центра ГосСОПКА: Сотрудник центра ГосСОПКА, осуществляющий обеспечение функционирования средств, размещаемых в центре ГосСОПКА, а также дополнительных средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

10 **специалист по оценке защищенности:** Сотрудник, осуществляющий анализ возможности использования обнаруженных уязвимостей информационного ресурса для реализации компьютерных атак.

11 **специалист по реагированию на компьютерные инциденты (центра ГосСОПКА):** Сотрудник центра ГосСОПКА, осуществляющий координацию действий по локализации компьютерного инцидента, выявлению и ликвидации его последствий (приведению информационной инфраструктуры (ИИ) в штатный режим работы (функционирования)).

12 **специалист по установлению причин компьютерных инцидентов (центра ГосСОПКА):** Сотрудник центра ГосСОПКА, осуществляющий анализ компьютерных инцидентов с целью уста-

новления причин их возникновения, анализ последствий инцидентов и подготовку перечня компьютерных инцидентов для представления в НКЦКИ.

13 **аналитик (центра ГосСОПКА):** Сотрудник центра ГосСОПКА, осуществляющий анализ информации о зарегистрированных компьютерных инцидентах, анализ возможностей реализации угроз, связанных с компьютерными атаками, оценку обстановки, прогнозирование развития угроз реализации компьютерных атак, разработку рекомендаций по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов.

14 **технический эксперт (центра ГосСОПКА):** Сотрудник центра ГосСОПКА, осуществляющий экспертную поддержку в соответствии со специализацией (вредоносное программное обеспечение, применение специализированных технических средств, оценка защищенности и т.п.), формирование предложений по устранению в информационных ресурсах причин и условий возникновения компьютерных инцидентов.

15 **специалист [методист] (центра ГосСОПКА):** Сотрудник центра ГосСОПКА, осуществляющий нормативно-правовое и методическое сопровождение деятельности центра ГосСОПКА.

16 **руководитель (центра ГосСОПКА):** Сотрудник центра ГосСОПКА, осуществляющий управление деятельностью центра ГосСОПКА, а также организующий взаимодействие с НКЦКИ, внесение изменений в соответствующие локальные нормативные акты и методические документы организации.

Средства государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

17 **средства государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;** средства ГосСОПКА: Технические, программные, программно-аппаратные и иные средства для обнаружения компьютерных атак, технические, программные, программно-аппаратные и иные средства для предупреждения компьютерных атак, технические, программные, программно-аппаратные и иные средства для ликвидации последствий компьютерных атак, технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи, технические, программные, программно-аппаратные и иные средства обмена информацией, для которых имеется документальное подтверждение соответствия требованиям, установленным в нормативных правовых актах и методических документах ФСБ России.

Примечание — С учетом определений, представленных в 18—22.

18 **технические, программные, программно-аппаратные и иные средства для обнаружения компьютерных атак;** средства обнаружения: Средства, предназначенные для управления сбором и анализом данных о регистрируемых событиях ИБ и иных данных с целью своевременного выявления компьютерных инцидентов, произошедших в том числе в результате компьютерных атак.

Примечание — Средства обнаружения реализуют функции по управлению событиями ИБ для обнаружения реализации компьютерных атак и другие функции в соответствии с нормативными правовыми актами и методическими документами ФСБ России. В качестве средств обнаружения могут, например, использоваться средства управления событиями ИБ.

19 **технические, программные, программно-аппаратные и иные средства для предупреждения компьютерных атак;** средства предупреждения: Средства, предназначенные для сбора и обработки сведений, необходимых для формирования рекомендаций, направленных на ликвидацию, снижение вероятности реализации и тяжести последствий компьютерных атак.

20 **технические, программные, программно-аппаратные и иные средства для ликвидации последствий компьютерных атак;** средства ликвидации последствий: Средства, предназначенные для управления процессами регистрации компьютерных инцидентов, произошедших в том числе в результате компьютерных атак, а также управления процессами реагирования на компьютерные инциденты.

Примечание — Средства ликвидации последствий реализуют функции по управлению компьютерными инцидентами для ликвидации последствий компьютерных атак и другие функции в соответствии с нормативными правовыми актами и методическими документами ФСБ России. В качестве средств ликвидации последствий могут выступать средства управления инцидентами.

21 **технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи;** средства ППКА: Средства, предназначенные для обнаружения в сетях электросвязи, используемых для организации взаимодействия информационных

ресурсов, признаков компьютерных атак по значениям служебных полей протоколов сетевого взаимодействия, а также осуществления сбора, накопления и статистической обработки результатов такого обнаружения.

22 **технические, программные, программно-аппаратные и иные средства обмена информацией;** средства обмена: Средства, предназначенные для обеспечения передачи, приема и целостности при передаче и приеме информации, необходимой субъектам ГосСОПКА при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак и реагировании на компьютерные инциденты.

Информационные ресурсы

23 **информационная инфраструктура (субъекта ГосСОПКА);** ИИ: Информационные ресурсы, а также сети электросвязи, используемые для организации их взаимодействия.

24 **информационные ресурсы (входящие в зону ответственности субъекта ГосСОПКА):** Информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления.

25 **элементы информационной инфраструктуры (субъекта ГосСОПКА),** элементы ИИ: Программно-технические средства (средства вычислительной техники), обладающие функциями хранения, обработки и (или) передачи информации, входящие в состав ИИ.

Компьютерные атаки и компьютерные инциденты

26

инцидент информационной безопасности; инцидент ИБ: Непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (могут привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации.

[Адаптировано из [2], приложение № 1]

27 **компьютерный инцидент:** Факт нарушения и (или) прекращения функционирования информационного ресурса, сети электросвязи, используемой для организации взаимодействия информационных ресурсов, и (или) нарушения безопасности обрабатываемой в информационном ресурсе информации, в том числе произошедший в результате компьютерной атаки.

Примечание — Компьютерные инциденты представляют собой подмножество инцидентов ИБ, которое характеризуется подтвержденным фактом нарушения и (или) прекращения функционирования информационного ресурса, сети электросвязи, используемой для организации взаимодействия информационных ресурсов, и (или) нарушения безопасности обрабатываемой в информационном ресурсе информации.

28 **карточка компьютерного инцидента:** Документ установленной формы, предназначенный для формализованного описания компьютерных инцидентов.

29 **тип компьютерного инцидента:** Классификация разновидностей компьютерных инцидентов.

30 **компьютерная атака:** Целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и (или) создания угрозы безопасности обрабатываемой таким ресурсом информации.

31 **источник компьютерной атаки:** Лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

32 **тактика (проведения компьютерной атаки):** Совокупность приемов и способов действий, используемых для проведения компьютерной атаки.

33 **техника (проведения компьютерной атаки):** Совокупность и порядок действий, используемых для проведения компьютерной атаки в рамках соответствующих тактик.

34 **тип компьютерной атаки:** Классификация разновидностей компьютерных атак.

Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты

35

мониторинг информационной безопасности; мониторинг ИБ: Процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей.

[ГОСТ Р 59547—2021, пункт 3.7]

Примечание — Деятельность по обнаружению и регистрации компьютерных инцидентов основывается на результатах проводимого в организации мониторинга, в рамках которого осуществляется сбор информации о событиях ИБ и иных данных мониторинга из различных источников.

36

данные мониторинга: Данные о состоянии объектов мониторинга ИБ, а также данные, получаемые из среды функционирования объекта мониторинга и внешних сервисов, которые могут использоваться для выявления уязвимостей и угроз безопасности информации.

[ГОСТ Р 59547—2021, пункт 3.2]

Примечания

1 К данным мониторинга могут относиться данные о событиях ИБ, выявленных уязвимостях, результатах контроля соответствия конфигурационных настроек; действиях пользователей; результатах контроля потоков информации, работоспособности программных, технических и программно-технических средств, включая средства защиты информации, а также различные справочные данные.

2 В деятельности по управлению компьютерными инцидентами данные мониторинга могут использоваться с целью анализа возможности использования уязвимостей информационного ресурса для реализации компьютерных атак, анализа угроз по реализации компьютерных атак и выявления и регистрации компьютерных инцидентов.

37

событие (информационной) безопасности: Зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой средств ЗИ, или ситуацию, которая может быть значимой для безопасности информации.

[ГОСТ Р 59547—2021, пункт 3.13]

38

индикатор компрометации: Известные данные, указывающие на то, что безопасность объекта мониторинга уже нарушена.

[ГОСТ Р 59547—2021, пункт 3.3]

39 **управление компьютерным инцидентом:** Деятельность, направленная на обнаружение и регистрацию, анализ и реагирование на компьютерный инцидент, а также использование полученного при этом опыта для предотвращения повторного возникновения компьютерного инцидента, повышения эффективности процедур реагирования на компьютерный инцидент.

40 **обнаружение компьютерных атак:** Комплекс мероприятий по выявлению и анализу признаков компьютерных атак и определению их типа.

41 **регистрация компьютерного инцидента:** Процесс (процедура, функция) фиксации сведений о компьютерном инциденте по установленной форме.

42 **реагирование на компьютерный инцидент:** Последовательное выполнение этапов реагирования на компьютерный инцидент с целью установления технических причин и условий возникновения компьютерного инцидента и ликвидации его последствий.

43 **этап реагирования (на компьютерный инцидент):** Действие или совокупность действий, осуществляемых по отношению к зарегистрированному компьютерному инциденту.

44 **план реагирования (на компьютерный инцидент):** Набор документированных процедур и инструкций, определяющих порядок реализации мероприятий по реагированию на компьютерные инциденты.

45 **время реагирования (на компьютерный инцидент):** Время реакции на инцидент, характеризующее интервал между получением информации о возникновении компьютерного инцидента и моментом закрытия компьютерного инцидента.

46 **локализация компьютерного инцидента:** Совокупность действий, направленных на определение и ограничение функционирования информационных ресурсов, на которых обнаружены признаки зарегистрированного компьютерного инцидента, с целью предотвращения его дальнейшего распространения.

47 **выявление последствий компьютерного инцидента:** Совокупность действий, направленных на определение фактов несанкционированного раскрытия, модификации, уничтожения информации или блокирования доступа к ней, а также фактов внесения нарушителем ИБ в информационный ресурс изменений, позволяющих ему осуществлять дальнейшие несанкционированные действия по отношению к защищаемой информации, связанных с зарегистрированным компьютерным инцидентом.

Примечание — В качестве фактов внесения в информационный ресурс изменений следует рассматривать: создание нарушителем ИБ нелегитимной учетной записи пользователя, внедрение в информационный ресурс нештатного программного обеспечения, изменение настроек средств защиты информации и программного обеспечения, а также другие изменения, вносимые нарушителем ИБ в информационный ресурс с целью использования их для осуществления дальнейших несанкционированных действий по отношению к защищаемой информации.

48 **ликвидация последствий компьютерного инцидента:** Совокупность действий, направленных на восстановление штатного режима функционирования информационных ресурсов после компьютерного инцидента и удаление изменений, внесенных нарушителем ИБ в информационный ресурс.

49 **установление причин компьютерного инцидента:** Совокупность действий, направленных на определение факторов, обусловивших возможность возникновения компьютерного инцидента и (или) способствовавших его возникновению.

50 **закрытие компьютерного инцидента:** Совокупность действий, направленных на проверку результатов выполнения мероприятий (этапов) реагирования на компьютерный инцидент для принятия решения о его закрытии или о необходимости проведения дополнительных действий по реагированию.

51 **принятие мер по предотвращению повторного возникновения компьютерных инцидентов:** Реализация мер защиты информации, обеспечивающих противодействие (снижение вероятности вплоть до недопущения) повторному возникновению компьютерных инцидентов.

52

восстановление: Процесс и событие, заключающиеся в переходе объекта из неработоспособного состояния в работоспособное состояние.

[ГОСТ 27.102—2021, статья 65]

53

время восстановления: Время, затрачиваемое непосредственно на выполнение операций по восстановлению объекта.

[ГОСТ 27.102—2021, статья 32]

54 **инвентаризация информационного ресурса:** Деятельность, направленная на сбор информации об информационном ресурсе, включая используемые в нем технические, программные и (или) программно-аппаратные средства (программно-технические средства).

55 **решающее правило обнаружения [сигнатура] компьютерной атаки (средства обнаружения компьютерных атак; системы обнаружения вторжений):** Совокупность характерных признаков компьютерной атаки, на основе которой средство обнаружения компьютерных атак (система обнаружения вторжений) принимает решение об обнаружении определенной компьютерной атаки.

56

база решающих правил (средства обнаружения компьютерных атак; системы обнаружения вторжений): База, содержащая решающие правила обнаружения компьютерной атаки (сигнатуры), с использованием которой средство обнаружения компьютерных атак (система обнаружения вторжений) осуществляет регистрацию признаков различных компьютерных атак.

[Адаптировано из [3], раздел 1, подраздел 1.5]

57 **предупреждение компьютерных атак:** Комплекс превентивных мероприятий, направленных на повышение защищенности информационных ресурсов от компьютерных атак.

58 **индикатор вредоносной активности:** Известные данные, указывающие на факт нарушения безопасности информационного ресурса, либо данные, описывающие события ИБ, которые несут угрозу нарушения его безопасности.

59 **бюллетень безопасности:** Официальное заявление об угрозах безопасности информации, возникающих при эксплуатации программных или программно-аппаратных средств, с раскрытием информации о соответствующих уязвимостях и (или) содержащее рекомендации по устранению данных угроз.

60 **атрибуция (компьютерных атак):** Предполагаемое соотнесение используемых тактик, техник и средств проведения компьютерных атак с нарушителями.

61 **оценка степени защищенности от компьютерных атак:** Процесс анализа возможности использования обнаруженных уязвимостей информационного ресурса для реализации компьютерных атак.

62 **источник данных для выявления признаков возможного возникновения компьютерных инцидентов:** Программное или программно-аппаратное средство, осуществляющее регистрацию событий ИБ и иных данных мониторинга, которые могут использоваться для выявления признаков возможного возникновения компьютерных инцидентов.

Алфавитный указатель терминов

аналитик 13
аналитик центра ГосСОПКА 13
атака компьютерная 30
атрибуция 60
атрибуция компьютерных атак 60
база решающих правил 56
база решающих правил системы обнаружения вторжений 56
база решающих правил средства обнаружения компьютерных атак 56
бюллетень безопасности 59
восстановление 52
время восстановления 53
время реагирования 45
время реагирования на компьютерный инцидент 45
выявление последствий компьютерного инцидента 47
государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации 1
данные мониторинга 36
закрытие компьютерного инцидента 50
зона ответственности 5
зона ответственности субъекта ГосСОПКА 5
инвентаризация информационного ресурса 54
индикатор вредоносной активности 58
индикатор компрометации 38
инфраструктура информационная 23
инфраструктура информационная субъекта ГосСОПКА 23
инцидент компьютерный 27
инцидент ИБ 26
инцидент информационной безопасности 26
источник данных для выявления признаков возможного возникновения компьютерных инцидентов 62
источник компьютерной атаки 31
карточка компьютерного инцидента 28
ликвидация последствий компьютерного инцидента 48
локализация компьютерного инцидента 46
методист 15
методист центра ГосСОПКА 15
мониторинг ИБ 35
мониторинг информационной безопасности 35
национальный координационный центр по компьютерным инцидентам 4
обнаружение компьютерных атак 40
оценка степени защищенности от компьютерных атак 61
план реагирования 44
план реагирования на компьютерный инцидент 44
правило обнаружения компьютерной атаки решающее 55
правило обнаружения компьютерной атаки решающее средства обнаружения компьютерных атак 55

правило обнаружения компьютерной атаки решающее системы обнаружения вторжений 55
предупреждение компьютерных атак 57
принятие мер по предотвращению повторного возникновения компьютерных инцидентов 51
реагирование на компьютерный инцидент 42
регистрация компьютерного инцидента 41
ресурсы информационные 24
ресурсы информационные входящие в зону ответственности субъекта 24
руководитель 16
руководитель центра ГосСОПКА 16
сигнатура компьютерной атаки 55
сигнатура компьютерной атаки средства обнаружения компьютерных атак 55
сигнатура компьютерной атаки системы обнаружения вторжений 55
силы госСОПКА 2
силы государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации 2
событие безопасности 37
событие информационной безопасности 37
специалист 15
специалист центра ГосСОПКА 15
специалист по взаимодействию с персоналом и пользователями 7
специалист по взаимодействию с персоналом и пользователями центра ГосСОПКА 7
специалист по реагированию на компьютерные инциденты 11
специалист по реагированию на компьютерные инциденты центра ГосСОПКА 11
специалист по обнаружению компьютерных атак и инцидентов 8
специалист по обнаружению компьютерных атак и инцидентов центра ГосСОПКА 8
специалист по обслуживанию средств центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации 9
специалист по оценке защищенности 10
специалист по установлению причин компьютерных инцидентов 12
специалист по установлению причин компьютерных инцидентов центра ГосСОПКА 12
средства ГосСОПКА 17
средства государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации 17
средства для ликвидации последствий компьютерных атак технические, программные, программно-аппаратные и иные 20
средства для обнаружения компьютерных атак технические, программные, программно-аппаратные и иные 18
средства для предупреждения технические, программные, программно-аппаратные и иные 19
средства обмена 22
средства обмена информацией технические, программные, программно-аппаратные и иные 22
средства поиска признаков компьютерных атак в сетях электросвязи технические, программные, программно-аппаратные и иные 21
средства ППКА 21

субъекты ГосСОПКА 3
субъекты государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации 3
тактика 32
тактика проведения компьютерной атаки 32
техника 33
техника проведения компьютерной атаки 33
тип компьютерного инцидента 29
тип компьютерной атаки 34
управление компьютерным инцидентом 39
установление причин компьютерного инцидента 49
центр государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации 6
эксперт технический 14
эксперт центра ГосСОПКА технический 14
элементы ИИ 25
элементы информационной инфраструктуры 25
элементы информационной инфраструктуры субъекта ГосСОПКА 25
этап реагирования 43
этап реагирования на компьютерный инцидент 43

Приложение А
(справочное)

Классификационные схемы понятий предметной области «Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирования на компьютерные инциденты»

А.1 Структура разделов стандарта показана на рисунке А.1.

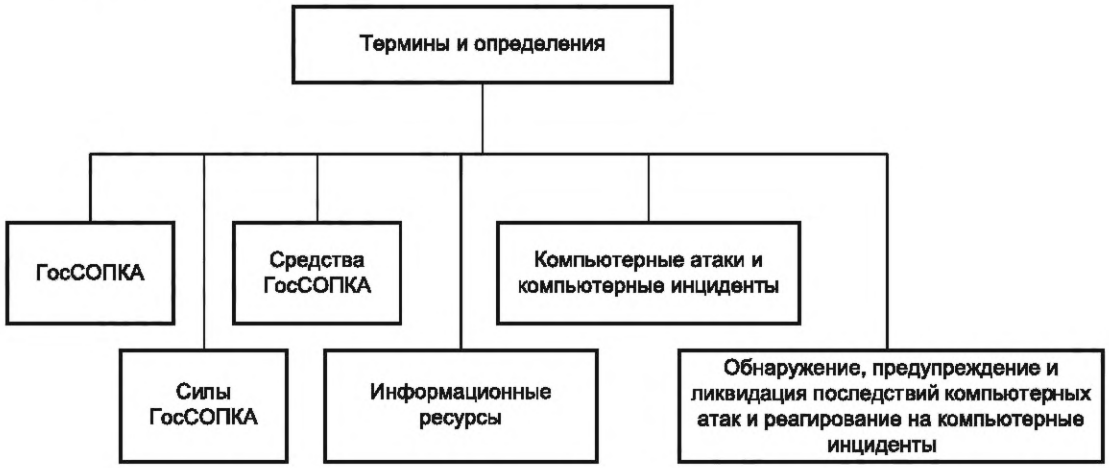

Рисунок А.1

А.2 Взаимосвязь терминов, определенных в подразделе «Силы государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», показана на рисунке А.2.

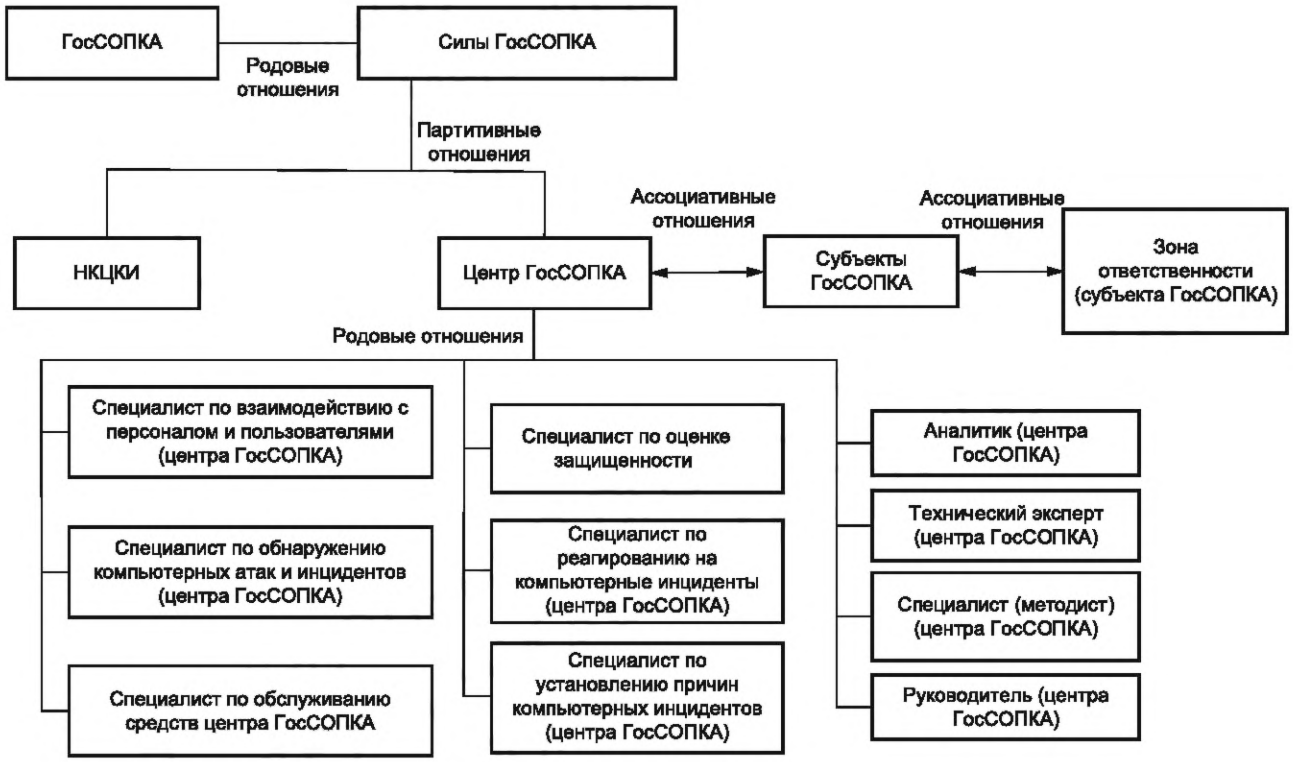

Рисунок А.2

А.3 Взаимосвязь терминов, определенных в подразделе «Средства государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», показана на рисунке А.3.



Рисунок А.3

А.4 Взаимосвязь терминов, определенных в подразделе «Информационные ресурсы», показана на рисунке А.4.

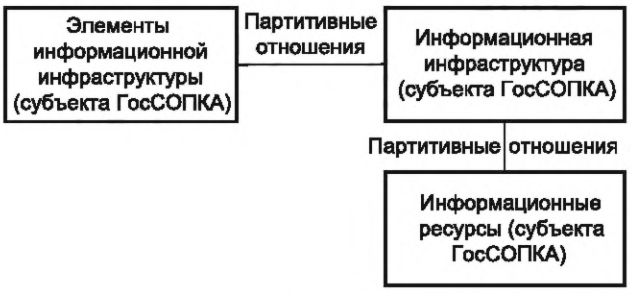

Рисунок А.4

А.5 Взаимосвязь терминов, определенных в подразделе «Компьютерные атаки и компьютерные инциденты», показана на рисунке А.5.

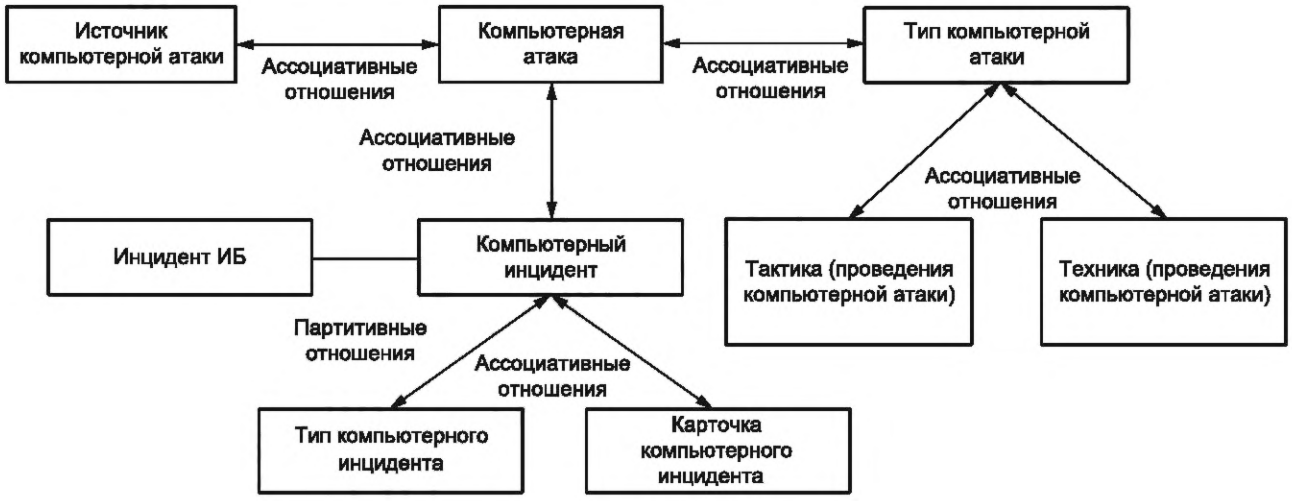

Рисунок А.5

А.6 Взаимосвязь терминов, определенных в подразделе «Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты», показана на рисунках А.6 и А.7.

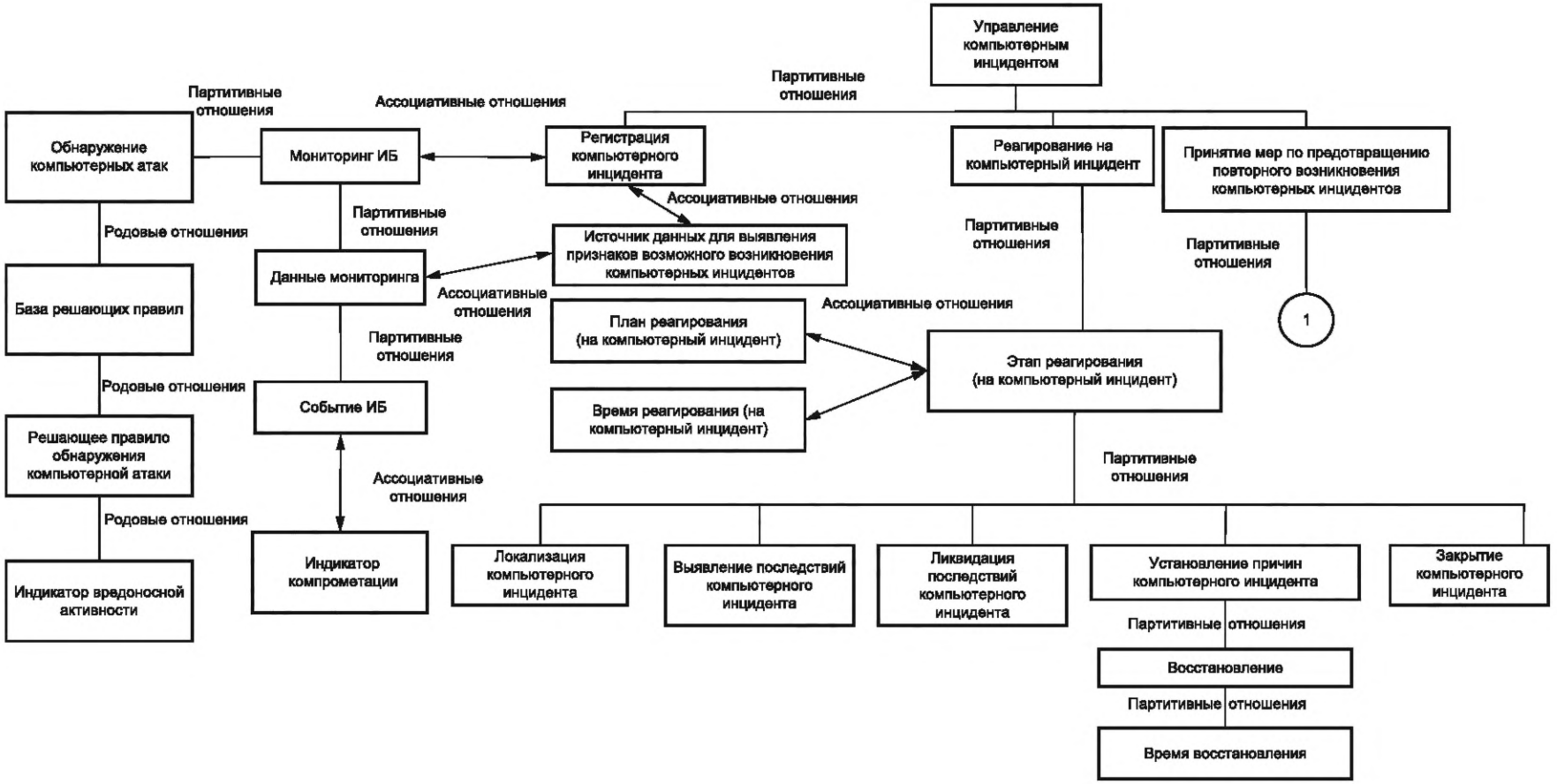

Рисунок А.6

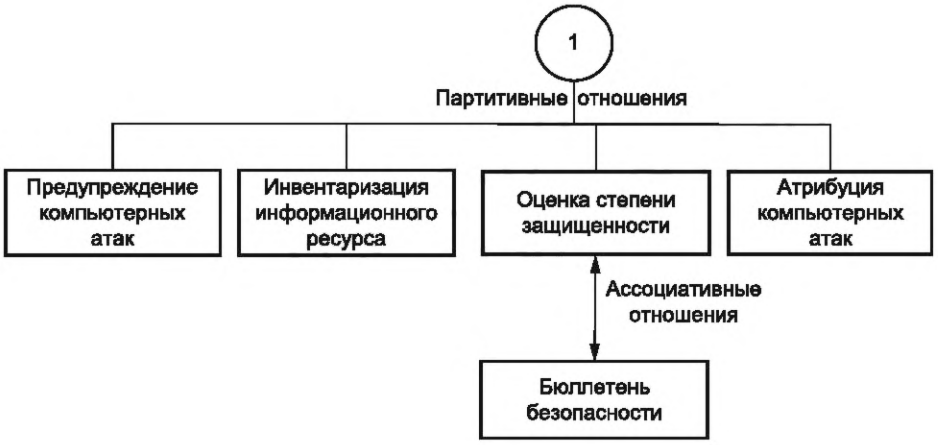
1
Партитивные отношения
Предупреждение компьютерных атак
Инвентаризация информационного ресурса
Оценка степени защищенности
Атрибуция компьютерных атак
Ассоциативные отношения
Бюллетень безопасности

Рисунок А.7

Библиография

[1] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[2] Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», 11.02.2014 г.

[3] Методические документы ФСТЭК России «Профили защиты систем обнаружения вторжений»

УДК 004.622:006.354 ОКС 35.020

Ключевые слова: компьютерная атака, компьютерный инцидент, управление компьютерным инцидентом, обнаружение компьютерных атак, регистрация компьютерного инцидента, реагирование на компьютерный инцидент

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 30.11.2022. Подписано в печать 07.12.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,12.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru