ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59547— 2021

Защита информации

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2021

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), 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 27 июля 2021 г. № 656-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 «РСТ», 2021

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
4 Общие положения 3
5 Требования к мониторингу информационной безопасности 6

Введение

Мониторинг ИБ в информационных системах и автоматизированных системах (далее — информационные (автоматизированные) системы) представляет собой процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей.

Процесс мониторинга ИБ может охватывать все или часть информационных (автоматизированных) систем, составляющих информационную инфраструктуру обладателя информации и (или) оператора, в том числе функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры.

В процессе мониторинга ИБ в рамках анализа результатов регистрации событий безопасности и иных данных мониторинга осуществляются:

- анализ событий безопасности и иных данных мониторинга;
- контроль (анализ) защищенности информации;
- анализ и оценка функционирования систем ЗИ информационных (автоматизированных) систем;
- периодический анализ изменения угроз безопасности информации в информационных (автоматизированных) системах, возникающих в ходе эксплуатации.

В настоящем стандарте определены:

а) требования к уровням мониторинга ИБ:
- к источникам данных мониторинга,
- сбору данных мониторинга,
- хранению, агрегированию и обработке данных мониторинга,
- представлению данных о результатах мониторинга;

б) порядок осуществления мониторинга ИБ при реализации мер ЗИ;

в) требования к защите данных мониторинга.

Мониторинг ИБ можно осуществлять в рамках системы менеджмента ИБ операторов информационных (автоматизированных) систем.

При осуществлении мониторинга ИБ могут быть использованы соответствующие автоматизированные средства (дополнительные программные и программно-технические средства).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общие положения

Information protection. Information security monitoring. General provisions

Дата введения — 2022—04—01

1 Область применения

Настоящий стандарт устанавливает уровни мониторинга ИБ, требования к каждому уровню, порядок осуществления мониторинга ИБ и требования к защите данных мониторинга.

Положения настоящего стандарта применимы к мероприятиям по мониторингу ИБ, осуществляемым операторами по отношению к эксплуатируемым ими информационным (автоматизированным) системам, а также к мероприятиям по мониторингу ИБ, осуществляемым в рамках деятельности по оказанию услуг мониторинга ИБ.

Настоящий стандарт не устанавливает требования к средствам мониторинга ИБ и к мероприятиям, связанным с выявлением компьютерных инцидентов и реагированием на них.

Примечание — Под мероприятиями мониторинга ИБ подразумевается совокупность действий, направленных на достижение целей мониторинга ИБ.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ Р 59548 Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации

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

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **агрегирование:** Процесс объединения однородных и повторяющихся данных о событиях безопасности или иных данных, получаемых в результате мониторинга ИБ.

Издание официальное

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

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

3.4 **источники данных мониторинга:** Программные или программно-технические средства, с которых может быть осуществлен сбор данных мониторинга.

3.5 **компенсирующие меры:** Меры защиты информации, которые применяются в информационной (автоматизированной) системе взамен отдельных мер защиты информации, подлежащих реализации в соответствии с предъявляемыми к информационной (автоматизированной) системе требованиями по защите информации, в связи с невозможностью их реализации.

Примечание — Компенсирующие меры должны быть достаточными для адекватного блокирования (нейтрализации) угроз безопасности информации.

3.6 **меры защиты информации:** Принятые правила, процедуры или механизмы, направленные на защиту информации.

3.7 **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.

3.8 **нарушение безопасности информации** (в информационных (автоматизированных) системах): Совокупность событий безопасности и (или) иных данных мониторинга, указывающая на возможное нарушение конфиденциальности, целостности и доступности информации, нарушение принятой политики безопасности или наличие уязвимости.

3.9 **нормализация (данных мониторинга):** Приведение получаемых от различных источников данных мониторинга к формату, необходимому для дальнейшей их обработки и хранения.

3.10 **объект мониторинга:** Объект или процесс, изменение состояния которого может привести к нарушению безопасности информации.

3.11 **оператор информационных [автоматизированных] систем**: Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационных (автоматизированных) систем, в том числе по обработке информации, содержащейся в базах данных.

3.12 **поток данных об угрозах, содержащий индикаторы компрометации:** Используемый при осуществлении мониторинга набор индикаторов компрометации, получаемый из источника, распространяющего сведения о выявленных индикаторах компрометации.

3.13 **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.

3.14 **угроза (безопасности информации):** Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
[ГОСТ Р 50922—2006, Статья 2.6.1]

3.15 **узел информационной [автоматизированной] системы:** Программно-техническое средство, предназначенное для выполнения определенных функций в составе информационной (автоматизированной) системы.

3.16 **уязвимость:** Свойство информационной (автоматизированной) системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

3.17 **фильтрация событий безопасности:** Выборка данных о событиях безопасности информации из состава данных, передаваемых для дальнейшего мониторинга ИБ или долгосрочного хранения по определенным критериям (правилам) мониторинга ИБ.

Примечание — Фильтрацию проводят с целью исключения из состава обрабатываемых данных мониторинга ИБ данных, не содержащих полезной информации, которую можно было бы использовать для достижения целей мониторинга.

4 Общие положения

4.1 При осуществлении мониторинга ИБ должна обеспечиваться возможность получения информации о зарегистрированных событиях безопасности и иных данных, необходимых для мониторинга ИБ, от различных источников, таких как средства ЗИ, ПО, программно-технические средства, информационные сервисы, среда функционирования информационных (автоматизированных) систем, работники (сотрудники) оператора информационных (автоматизированных) систем и иные источники данных.

Примечание — Под информационными сервисами понимаются услуги внешних информационных (автоматизированных) систем по предоставлению данных, которые могут использоваться для мониторинга ИБ (например, сервисы, предоставляющие данные об идентификаторах компрометации).

4.2 В рамках мероприятий по мониторингу ИБ решают следующие задачи:

а) в части мероприятий анализа событий безопасности и иных данных мониторинга:

1) сбор данных о событиях безопасности и иных данных мониторинга от различных источников,

2) нормализация, фильтрация и агрегирование данных о событиях безопасности,

3) анализ событий безопасности и иных данных мониторинга,

4) сопоставление событий безопасности с потоками данных, содержащих индикаторы компрометации,

5) контроль, учет и анализ действий пользователей и администраторов,

6) сбор и анализ данных о результатах контроля потоков информации,

7) выявление нарушений безопасности информации,

8) выявление скрытых уязвимостей путем сопоставления результатов регистрации событий безопасности с результатами анализа уязвимостей,

9) своевременное информирование ответственных лиц о выявленных нарушениях безопасности информации;

б) в части мероприятий контроля (анализа) защищенности информации:

1) выявление (поиск) уязвимостей,

2) разработка описаний выявленных уязвимостей,

3) контроль установки обновлений безопасности ПО, включая ПО средств ЗИ,

4) контроль состава программно-технических средств, виртуального аппаратного обеспечения, ПО и средств ЗИ (инвентаризация),

5) контроль соответствия настроек ПО и средств ЗИ установленным требованиям к защите информации (политикам безопасности),

6) информирование ответственных лиц о результатах поиска уязвимостей, контроля установки обновлений ПО, контроля состава программно-технических средств, ПО и средств ЗИ;

в) в части мероприятий анализа и оценки функционирования систем ЗИ информационных (автоматизированных) систем:

1) контроль работоспособности (неотключения) ПО и средств ЗИ,

2) проверка соответствия среды функционирования требованиям, предъявленным в документации на средства ЗИ,

3) контроль потоков информации, влияющих на производительность информационных (автоматизированных) систем, при межсетевом взаимодействии,

4) информирование о неисправностях, сбоях и отказах в функционировании средств и систем ЗИ информационных (автоматизированных) систем;

г) в части мероприятий периодического анализа изменения угроз безопасности информации в информационных (автоматизированных) системах, возникающих в ходе эксплуатации:

1) получение новых данных об индикаторах компрометации, уязвимостях и угрозах безопасности информации из доступных источников,

2) выявление новых угроз безопасности информации по результатам анализа событий безопасности и нарушений безопасности информации (например, свидетельствующих о нетипичной активности пользователей), выявленных в процессе мониторинга ИБ,

3) разработка требований к сбору, обработке, хранению и представлению данных о событиях безопасности и иных данных мониторинга от различных источников с учетом изменения угроз безопасности информации и новых данных об индикаторах компрометации и уязвимостях,

4) разработка новых и уточнение действующих правил анализа событий безопасности и иных данных мониторинга, используемых для выявления нарушений безопасности информации,

5) разработка рекомендаций по реализации дополнительных мер и мероприятий ЗИ, направленных на минимизацию существующих и выявление новых угроз безопасности.

4.3 Объектами мониторинга являются:

- автоматизированные рабочие места;
- серверное оборудование;
- телекоммуникационное оборудование;
- технологическое и (или) производственное оборудование (исполнительные устройства);
- средства ЗИ;
- иные объекты мониторинга, определенные оператором информационных (автоматизированных) систем.

4.4 Выделяются следующие уровни мониторинга ИБ:

- уровень источников данных;
- уровень сбора данных;
- уровень хранения, агрегирования и обработки данных;
- уровень представления информации и данных мониторинга.

Уровни мониторинга ИБ представлены на рисунке 1.

Примечание — Уровень мониторинга ИБ определяют совокупностью мероприятий с целью решения определенных задач.

4.5 При реализации мониторинга ИБ обеспечивается возможность реализации следующих свойств:

- многопараметричность — для обеспечения вертикальной интеграции процесса мониторинга ИБ в организационную структуру управления безопасностью организации, а также горизонтальной интеграции по структурным компонентам информационной инфраструктуры и информационных (автоматизированных) систем;
- масштабируемость — для расширения области мониторинга ИБ;
- адаптивность — для выявления новых видов, типов и способов осуществления компьютерных атак и иных видов нарушений безопасности информации за счет развития правил анализа событий безопасности и данных мониторинга;
- полнота — предполагает использование всех возможных источников событий безопасности и данных мониторинга, необходимых для выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей;
- доступность — предполагает обеспечение возможности получения данных мониторинга, необходимых для выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей в соответствии с заданными требованиями;
- достоверность — предполагает обеспечение возможности получения неискаженных (неподмененных) данных.

4.5.1 Реализация свойства многопараметричности обеспечивается применением необходимых форматов и способов сбора, обработки, хранения и представления данных мониторинга, которые позволяют интегрировать процесс мониторинга ИБ в организационную структуру управления безопасностью организации с учетом ее иерархии (вертикальная интеграция), а также осуществлять мониторинг нескольких информационных (автоматизированных) систем или объектов информационной инфраструктуры (горизонтальная интеграция).

4.5.2 Реализация свойства масштабируемости обеспечивается возможностью наращивания количества новых источников данных мониторинга ИБ, а также возможностью создания многоуровневой иерархической системы мониторинга ИБ.

4.5.3 Реализация свойств адаптивности обеспечивается наличием возможности добавления, удаления и изменения правил и процедур анализа данных мониторинга.

4.6 При осуществлении мониторинга ИБ обеспечивают:

- получение и обработку данных от множества, в том числе разнородных, источников данных мониторинга;
- представление результатов анализа данных мониторинга в режиме времени, близком к реальному;
- возможность анализа событий безопасности и иных данных мониторинга на основе различных правил;
- централизованное хранение данных мониторинга (для всех объектов мониторинга или в рамках каждого объекта мониторинга);
- возможность формирования различных отчетов по результатам мониторинга ИБ.

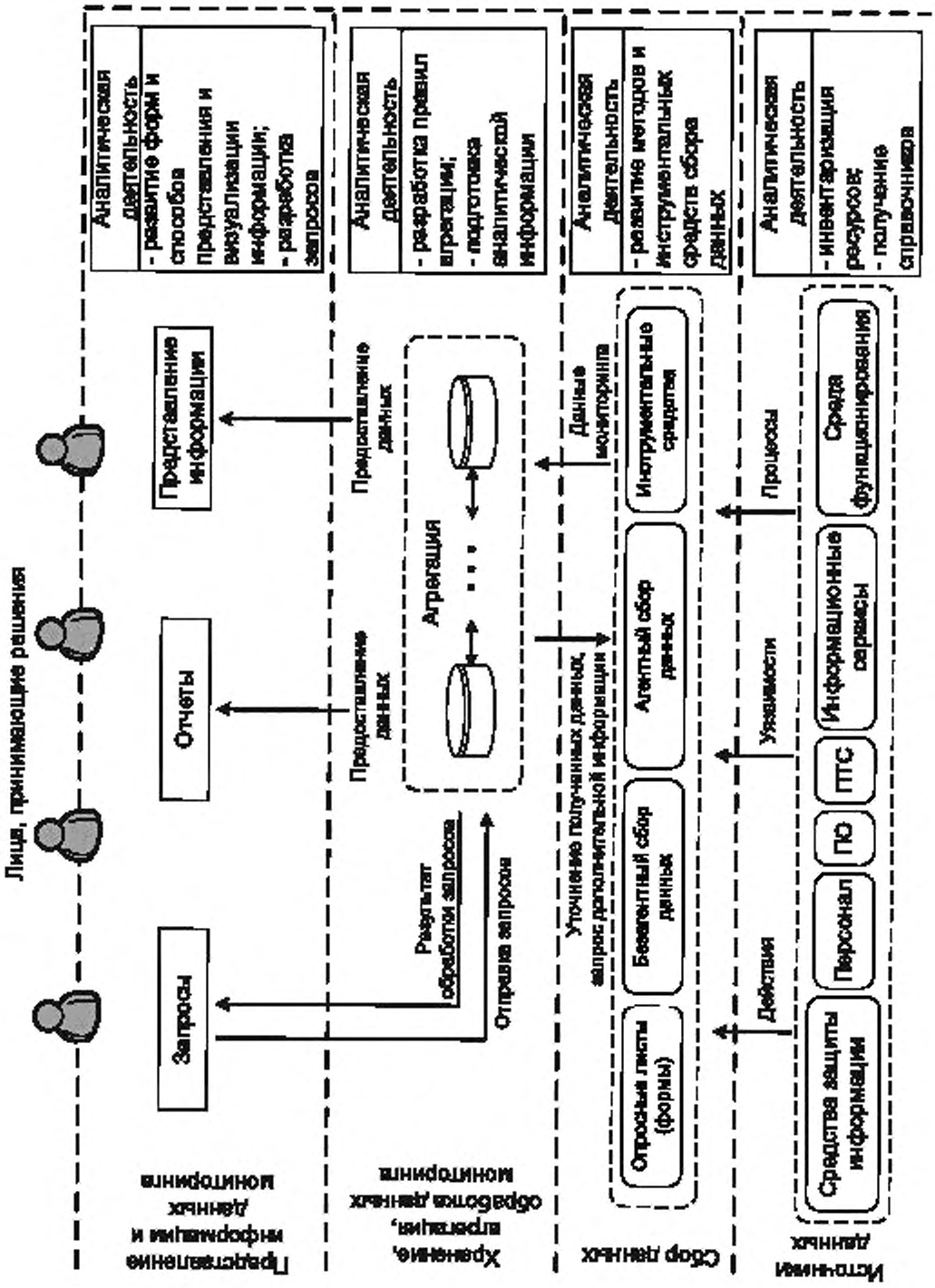


Рисунок 1 — Уровни мониторинга ИБ

5 Требования к мониторингу информационной безопасности

5.1 Требования к источникам данных

5.1.1 При осуществлении мониторинга ИБ данные мониторинга могут быть собраны с использованием как автоматизированных, так и неавтоматизированных средств.

Источниками данных мониторинга ИБ являются:

- средства ЗИ;
- ПО;
- программно-технические средства;
- информационные сервисы;
- среда функционирования информационных (автоматизированных) систем;
- оператор информационных (автоматизированных) систем;
- иные источники данных (в том числе внешние доступные источники данных).

5.1.2 При формировании перечня источников данных следует учитывать необходимость получения следующей информации:

а) данных о событиях безопасности от средств, осуществляющих регистрацию событий безопасности (источников событий безопасности);

б) данных о результатах выявления (поиска) уязвимостей, в том числе:

- в общесистемном (общем) ПО,
- прикладном ПО,
- специальном ПО,
- программно-технических средствах,
- портативных программно-технических средствах,
- коммуникационном (телекоммуникационном) оборудовании,
- средствах ЗИ;

в) данных о результатах контроля обновлений ПО, в том числе:

1) баз данных, необходимых для реализации функций безопасности средства ЗИ (обновление баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты, баз сигнатур уязвимостей средств контроля (анализа) защищенности, баз решающих правил систем обнаружения вторжений и других),

2) направленных на устранение уязвимостей средства (средств) ЗИ,

3) направленных на добавление функции (функций) безопасности средства (средств) ЗИ, на совершенствование реализации функции (функций) безопасности средства (средств) ЗИ, на расширение числа поддерживаемых программных и аппаратных платформ (если необходимость таких обновлений была определена по результатам анализа изменения угроз безопасности информации в информационных (автоматизированных) системах, возникающих в ходе их эксплуатации),

4) направленных на устранение уязвимостей общесистемного, прикладного и иного ПО;

г) данных о результатах контроля состава программно-технических средств, ПО и средств ЗИ (инвентаризационных данных), включая:

1) архитектуру информационных (автоматизированных) систем (сетевые адреса и имена),

2) местоположение узлов информационных (автоматизированных) систем,

3) назначение узлов информационных (автоматизированных) систем,

4) функционирующие сетевые службы,

5) сведения об источниках событий безопасности,

6) характеристики программно-технических средств, ПО и средств ЗИ,

7) принадлежность программно-технических средств подразделениям оператора информационных (автоматизированных) систем (сведения о владельцах),

8) принадлежность программно-технических средств соответствующим информационным (автоматизированным) системам,

9) конфигурацию узлов информационных (автоматизированных) систем;

д) данных о результатах контроля соответствия настроек ПО и средств ЗИ установленным требованиям к ЗИ (политикам безопасности);

е) данных о работоспособности (неотключении) ПО и средств ЗИ;

ж) информации о результатах контроля потоков информации, включая:

1) результаты контроля объемов сетевого трафика (входящего и исходящего) по различным типам протоколов и типам передаваемых файлов,

2) результаты контроля содержимого сетевого трафика по различным типам протоколов и файлов в целях выявления запрещенного или подозрительного контента и конфиденциальной информации,

3) результаты контроля потоков ввода/вывода информации при работе со съемными машинными носителями информации в целях выявления запрещенной деятельности, а также запрещенного или подозрительного контента и конфиденциальной информации,

4) результаты контроля вывода информации на печать,

5) результаты контроля подозрительной сетевой активности и выявления компьютерных атак или признаков подготовки к ним, а также несанкционированных действий пользователей в сети (например, попыток несанкционированного доступа пользователей к различным информационным ресурсам или подключения к сети посторонних устройств),

6) результаты контроля состояния беспроводных сетей в целях выявления несанкционированных подключений;

и) данных о действиях пользователей и процессов, необходимых для выявления преднамеренного или непреднамеренного нарушения установленных политик безопасности, регламентов работы, фактов запрещенной деятельности, попыток совершения несанкционированного доступа и утечки конфиденциальной информации, включая:

1) контроль запуска/останова различных процессов,

2) контроль подключения съемных машинных носителей информации и работы с ними,

3) контроль подключения мобильных, беспроводных и других устройств,

4) контроль установки/удаления ПО (компонентов ПО),

5) контроль изменения сетевых настроек автоматизированных рабочих мест и серверов,

6) контроль несанкционированных сетевых соединений с не разрешенными политикой безопасности сетевыми ресурсами,

7) контроль попыток удаленного доступа к автоматизированным рабочим местам и серверам,

8) контроль фактов работы с административными правами и полномочиями,

9) контроль изменения локальных политик безопасности, прав и привилегий,

10) контроль создания и работы с общими ресурсами,

11) контроль открытия «подозрительных» сетевых портов,

12) иные действия пользователей;

к) справочной информации, включая:

1) информацию о показателе доверия (репутации) сетевых адресов, доменных имен, серверов электронной почты, серверов доменных имен,

2) информацию о владельцах сетевых адресов, доменных имен, серверов электронной почты, серверов доменных имен,

3) информацию о местоположении и географической принадлежности сетевых адресов,

4) информацию об известных уязвимостях используемого ПО,

5) информацию о компьютерных сетях, состоящих из управляемых с использованием вредоносного ПО средств вычислительной техники, включая сведения об их управляющих серверах;

л) данных о новых угрозах безопасности информации.

5.1.3 При организации процесса мониторинга ИБ целесообразно выбирать источники данных, которые обеспечивают:

- передачу данных мониторинга ИБ (при наличии технической возможности) и возможность настройки состава передаваемых данных (предварительная фильтрация);

- предоставление справочников, содержащих описание идентификаторов отдельных типов данных (если справочники используются источником);

- предоставление данных мониторинга ИБ с описанием полей регистрируемых событий безопасности для последующей их интерпретации;

- предоставление данных мониторинга ИБ об уровне важности событий, которые могут быть использованы для обеспечения фильтрации событий;

- временное накопление событий безопасности (при наличии технической возможности) при отсутствии связи и их передачу при появлении связи с объектом назначения передачи данных мониторинга ИБ.

5.1.4 Источники данных о событиях безопасности могут предоставлять доступ к данным о событиях безопасности одним из следующих способов:

- предоставление источником данных доступа к файлам или базам данных журналов событий безопасности;
- выгрузка данных о событиях безопасности с использованием стандартных протоколов передачи данных;
- предоставление источником данных доступа к данным о событиях безопасности через программный интерфейс приложения или веб-сервис источника.

Примечание — Под веб-сервисом понимают идентифицируемую веб-адресом программную систему со стандартизированными интерфейсами.

5.1.5 Для источников данных операторами информационных (автоматизированных) систем обеспечивается достоверность передаваемых ими данных о дате и времени регистрации событий безопасности и, при необходимости, синхронизация системных часов с учетом часовых поясов.

5.2 Требования к сбору данных

5.2.1 При мониторинге ИБ осуществляют сбор исходных данных в объеме, необходимом и достаточном для проведения анализа и различного рода оценок состояния ИБ.

5.2.2 При использовании автоматизированных средств мониторинга для получения исходных данных можно применять:

- агентный сбор данных (агенты мониторинга событий безопасности);
- безагентный сбор данных;
- опросные листы (формы);
- инструментальные средства.

5.2.3 Агентом мониторинга событий безопасности является ПО, устанавливаемое на компонентах информационной инфраструктуры и узлах информационных (автоматизированных) систем с целью сбора необходимых данных непосредственно с источника.

5.2.4 С использованием агентов мониторинга может осуществляться сбор данных о событиях безопасности, о работоспособности (неотключении) ПО, о действиях пользователей и иных данных. При этом в составе агентов мониторинга могут быть реализованы отдельные функции инструментальных средств, которые позволяют дополнительно получать данные:

- о результатах контроля состава программно-технических средств, ПО и средств ЗИ (техническая инвентаризация);
- о результатах выявления (поиска) уязвимостей;
- о результатах контроля установки обновлений ПО;
- о результатах контроля соответствия настроек ПО и средств ЗИ установленным требованиям к ЗИ (политикам безопасности).

5.2.5 Безагентный сбор данных предполагает получение данных от источников по сети передачи данных без установки дополнительного ПО для сбора данных мониторинга. К методам безагентного сбора данных относятся:

- чтение данных непосредственно из файлов или баз данных журналов событий безопасности;
- прием данных, передаваемых от источников, с использованием стандартных протоколов передачи данных о событиях безопасности;
- сбор данных путем подключения к программному интерфейсу приложения или веб-сервису источника данных.

Безагентный сбор данных можно осуществлять как с использованием инструментальных средств, так и без применения инструментальных средств.

Без использования инструментальных средств сбор данных может осуществляться только путем чтения данных непосредственно из файлов или баз данных журналов событий безопасности с использованием пользовательского интерфейса для просмотра журналов источника или без использования указанного пользовательского интерфейса (если позволяет формат ведения журнала).

5.2.6 С использованием безагентного сбора данных можно осуществлять сбор данных о событиях безопасности, о работоспособности (неотключении) ПО и иных данных, которые может предоставить источник.

5.2.7 Сбор данных о событиях безопасности с использованием опросных листов (форм) осуществляют путем заполнения специальных электронных (бумажных) форм с последующей их передачей персоналу, осуществляющему мониторинг ИБ.

5.2.8 Сбор данных с использованием опросных листов (форм) включает:

- разработку опросного листа (формы), содержащего перечень необходимых данных с необходимым количеством полей;
- разработку регламента сбора и передачи данных о событиях безопасности персоналу, осуществляющему мониторинг ИБ;
- внедрение опросного листа (формы);
- регистрацию в опросных листах (формах) необходимых данных и последующую их передачу персоналу, осуществляющему мониторинг ИБ.

5.2.9 Выделяют два типа опросных листов (форм):

- периодически собираемые (например, результаты инвентаризации программно-технических средств, обновлений и пр.);
- постоянно действующие (например, опросные листы для сообщения о выявленном событии безопасности).

Примечание — Постоянно действующие опросные листы предназначены для оперативного доведения до персонала, осуществляющего мониторинг ИБ, информации о возможных нарушениях безопасности информации, признаки которых обнаружены пользователями. В связи с тем, что такие опросные листы требуют оперативного доведения информации до персонала, осуществляющего мониторинг, они реализуются только специализированными инструментальными средствами, которые предоставляют интерфейс, позволяющий пользователю сообщить сведения о выявленных им признаках возможного нарушения.

5.2.10 С использованием опросных листов (форм) можно передавать следующие данные мониторинга ИБ:

- о выявляемых событиях безопасности;
- составе программно-технических средств, ПО и средств ЗИ;
- результатах контроля установки обновлений ПО;
- результатах контроля соответствия настроек ПО и средств ЗИ установленным требованиям к ЗИ (политикам безопасности);
- иные данные и сведения, необходимые для мониторинга ИБ.

5.2.11 С использованием опросных листов (форм) передают данные мониторинга ИБ, которые невозможно передать каким-либо иным способом.

5.2.12 К инструментальным средствам сбора данных относятся:

- средства управления информацией об угрозах безопасности информации;
- замкнутые среды предварительного исполнения программ («песочницы»);
- средства (системы) контроля (анализа) защищенности;
- средства инвентаризации программно-технических средств, ПО и средств ЗИ.

5.2.13 Применение инструментальных средств для мониторинга ИБ позволяет получать и обрабатывать данные:

- о результатах контроля состава программно-технических средств, ПО и средств ЗИ (техническая инвентаризация);
- результатах выявления (поиска) уязвимостей;
- результатах контроля установки обновлений ПО;
- результатах контроля соответствия настроек ПО и средств ЗИ установленным требованиям к ЗИ (политикам безопасности);
- результатах выявления уязвимостей и угроз, оказывающих влияние на безопасность информации, полученных в результате проведения тестовых испытаний в замкнутых средах предварительного исполнения программ («песочницах»);
- новых угрозах безопасности информации.

Инструментальные средства применяют, если указанные данные не могут быть получены иным способом.

Примечание — Если в составе агента мониторинга реализована функция выявления (поиска) уязвимостей, применение дополнительных средств (систем) контроля (анализа) защищенности может не потребоваться. Примером реализации организационных мер может являться получение персоналом, осуществляющим монито-

ринг ИБ, информации о новых угрозах безопасности информации из доступных источников, содержащих сведения об уязвимостях и угрозах безопасности информации (например, банк данных угроз безопасности информации ФСТЭК России).

5.2.14 Для типов событий безопасности, определенных в ГОСТ Р 59548, мероприятия по мониторингу ИБ должны обеспечивать возможность получения регистрируемой информации, требования к составу которой определены в указанном национальном стандарте.

5.2.15 При сборе данных о событиях безопасности следует учесть необходимость получения:

- справочников, содержащих описание идентификаторов отдельных типов данных (если справочники используются источником);
- данных с описанием полей регистрируемых событий безопасности для последующей их интерпретации.

5.2.16 Мероприятия по мониторингу ИБ должны обеспечивать возможность фильтрации получаемых данных о событиях безопасности по уровню важности для обеспечения оперативной интеграции источников данных о событиях безопасности в процесс мониторинга ИБ и, при необходимости, по другим основаниям в соответствии с определенными правилами мониторинга ИБ.

Примечание — Фильтрация получаемых данных о событиях безопасности может также осуществляться на уровне хранения, агрегирования и обработки данных мониторинга, а также на уровне представления информации и данных мониторинга.

5.3 Требования к хранению, агрегированию и обработке данных мониторинга

5.3.1 Мероприятия по мониторингу ИБ должны обеспечивать хранение данных, собираемых от источников, и результатов их обработки.

5.3.2 Сроки и формат хранения данных о событиях безопасности должны обеспечивать возможность выявления и анализа возникших нарушений безопасности информации.

5.3.3 В рамках мероприятий по мониторингу ИБ реализуют следующие функции:

- нормализация полученных данных к формату, необходимому для дальнейшей их обработки и хранения;
- агрегирование данных (объединение нормализованных данных по группам на основе общих признаков);
- хранение агрегированных данных в течение срока хранения, определенного требованиями к ЗИ;
- анализ событий безопасности и иных данных мониторинга с целью выявления уязвимостей, угроз и нарушений безопасности информации;
- сопоставление событий безопасности с потоками данных об угрозах, содержащих индикаторы компрометации;
- сопоставление результатов регистрации событий безопасности с результатами анализа уязвимостей;
- выявление нарушений безопасности информации.

5.3.4 В рамках мероприятий по мониторингу ИБ также может быть реализовано хранение необработанных данных (до проведения их фильтрации, нормализации и (или) агрегирования).

5.3.5 В рамках мероприятий по мониторингу ИБ реализуют меры, направленные на предотвращение потери данных мониторинга. В качестве таких мер необходимо рассматривать:

- предупреждение (сигнализация, индикация) администратора при заполнении установленной части (процент или фактическое значение) объема памяти для хранения данных мониторинга;
- запись новых данных мониторинга ИБ поверх устаревших данных;
- архивирование (резервное копирование) данных мониторинга ИБ на съемные машинные носители информации, в сеть хранения данных, на специализированные устройства или на выделенные серверы.

5.3.6 С целью обеспечения возможности адаптации к новым типам угроз и их развивающимся методам в рамках мероприятий по мониторингу ИБ создают и актуализируют правила анализа событий безопасности и данных мониторинга, а также работники (сотрудники) оператора периодически оценивают актуальность новых угроз безопасности информации.

5.4 Требования к представлению данных о результатах мониторинга

5.4.1 В рамках мероприятий по мониторингу ИБ необходимо обеспечивать возможность представления как собранных данных о событиях безопасности и иных данных мониторинга, так и результатов выполнения определенных настоящим стандартом мероприятий мониторинга ИБ.

5.4.2 В рамках мероприятий по мониторингу ИБ необходимо обеспечивать возможность формирования следующих отчетов о результатах мониторинга ИБ:

- статистических, по собранным данным о событиях безопасности информации;
- о нарушениях безопасности информации, выявленных при анализе событий безопасности информации и иных данных мониторинга;
- с описанием выявленных уязвимостей;
- с собранными инвентаризационными данными;
- о результатах контроля соответствия настроек ПО и средств ЗИ установленным требованиям к ЗИ (политикам безопасности);
- о состоянии источников событий безопасности и данных.

5.4.3 На уровне представления информации и данных мониторинга ИБ нужно обеспечивать следующие условия:

- управление параметрами мониторинга и представление данных мониторинга, в том числе (при необходимости) с привязкой к объектам мониторинга;
- представление данных об объектах мониторинга, их состоянии и связях между ними;
- представление данных мониторинга ИБ в режиме времени, близком к реальному;
- представление данных мониторинга ИБ в соответствии с условиями выборки по установленным параметрам (запросами);
- представление данных мониторинга ИБ как в текстовом, так и в графическом виде.

Примечание — Под параметрами мониторинга понимают правила анализа данных мониторинга, используемые для выявления нарушений безопасности информации, и настройки автоматизированных средств, используемых для сбора данных мониторинга.

5.4.4 В рамках мероприятий по мониторингу ИБ необходимо обеспечивать информирование ответственных лиц о выявленных нарушениях безопасности информации, о результатах поиска уязвимостей контроля установки обновлений ПО и контроля состава программно-технических средств, о неисправностях ПО и средств ЗИ, сбоях и отказах в функционировании программно-технических средств. Информирование ответственных лиц может осуществляться путем отправки уведомлений по электронной почте, запуска внешнего приложения, используемого для оповещения, отображения сведений о событии безопасности в интерфейсе ПО, применяемого для мониторинга ИБ, и иными способами. В рамках оптимизации мероприятий по мониторингу ИБ должна быть предусмотрена возможность настройки оповещений (повторные оповещения, отсроченные оповещения, расширение перечня адресатов оповещений).

5.5 Порядок осуществления мониторинга информационной безопасности при реализации мер защиты информации

5.5.1 Мониторинг ИБ при реализации мер ЗИ проводят для всех событий, подлежащих регистрации, что обеспечивает своевременное выявление признаков нарушений безопасности информации.

5.5.2 Мероприятия по мониторингу ИБ можно применять для реализации мер ЗИ, связанных:

- с контролем состава программно-технических средств, ПО и средств ЗИ (инвентаризацией);
- регистрацией событий безопасности;
- выявлением (поиском) уязвимостей;
- контролем и анализом сетевого трафика;
- контролем использования интерфейсов ввода (вывода) информации на машинные носители информации;
- анализом действий пользователей;
- управлением конфигурацией информационных (автоматизированных) систем.

5.5.3 Мероприятия по мониторингу ИБ могут применяться как компенсирующие меры в случае технической сложности реализации или нецелесообразности применения иных мер ЗИ.

5.5.4 Для осуществления мероприятий по мониторингу ИБ должно быть обеспечено наличие штатного обученного персонала соответствующих категорий (ответственных лиц, дежурных смен), основной деятельностью которых является постоянный мониторинг ИБ.

Квалификация персонала, осуществляющего мониторинг ИБ, должна быть достаточной для выполнения возложенных на них функций.

Выделяют следующие роли для персонала, осуществляющего мониторинг ИБ, и их функции:

а) руководитель — выполняет функции, связанные с управлением персоналом, обеспечивающим функционирование процесса мониторинга ИБ;

б) системный администратор — выполняет функции, связанные с установкой и обеспечением работоспособности программных и аппаратных компонентов, применяемых для мониторинга ИБ, разработкой запросов на представление информации и данных мониторинга, а также с развитием форм представления и визуализации информации и данных мониторинга;

в) администратор безопасности — выполняет функции, связанные с организацией настройки программных и аппаратных компонентов, применяемых для мониторинга ИБ;

г) специалист по взаимодействию с персоналом и пользователями — выполняет функции, связанные с приемом и регистрацией сообщений персонала и пользователей о выявленных нарушениях безопасности информации;

д) оператор мониторинга — выполняет функции, связанные с анализом результатов мониторинга ИБ (событий безопасности) и подготовкой аналитической информации;

е) специалист по оценке защищенности — выполняет функции, связанные:

- с контролем состава программно-технических средств, ПО и средств ЗИ (инвентаризация),
- выявлением угроз безопасности информации и уязвимостей,
- контролем соответствия настроек ПО и средств ЗИ установленным требованиям к ЗИ (политикам безопасности),
- развитием методов и инструментальных средств сбора данных;

ж) аналитик — выполняет функции, связанные с анализом результатов мониторинга ИБ (событий безопасности) и разработкой правил агрегирования и анализа событий безопасности и данных мониторинга, а также определением критериев нарушений безопасности информации.

Примечание — Специалисты, выполняющие перечисленные роли, могут подразделяться по соответствующим уровням (линиям).

Допускается возлагать на одного работника из числа персонала, осуществляющего мониторинг ИБ, функции, относящиеся к разным ролям персонала, осуществляющего мониторинг ИБ.

Допускается передавать часть функций мониторинга ИБ сторонним организациям, имеющим лицензии на соответствующие виды деятельности.

5.5.5 Обработка и анализ поступающих данных мониторинга ИБ предусматривают не только выявление различных нарушений безопасности информации, но и использование результатов реагирования на выявленные нарушения безопасности информации с целью разработки новых и корректировки существующих правил анализа событий безопасности и данных мониторинга (добавление (удаление) дополнительных условий с целью повышения эффективности выявления нарушений безопасности информации или снижения количества регистрируемых ложных нарушений безопасности информации, использование дополнительных источников для получения недостающих исходных данных).

5.5.6 В рамках мероприятий по мониторингу ИБ может быть принято решение о создании единого координирующего центра мониторинга (ситуационного центра мониторинга ИБ), позволяющего контролировать качество организации процесса мониторинга, а также непрерывность и результативность процесса мониторинга ИБ в различных аспектах, включающих:

- полноту охвата мониторингом информационных (автоматизированных) систем (в первую очередь с точки зрения состава вовлеченных в мониторинг средств — источников событий и исходных данных);
- состав правил анализа событий безопасности и данных мониторинга, а также критериев нарушений безопасности информации;
- контроль работоспособности всех компонентов, участвующих в мониторинге ИБ.

5.5.7 Развитие мероприятий по мониторингу ИБ предусматривает постепенный переход от реактивного подхода при выявлении угроз и нарушений безопасности информации, когда ведется поиск ответных мер на выявленную угрозу и (или) нарушение безопасности информации, к проактивному подходу, при котором в процессе мониторинга ИБ выявляются предпосылки для реализации угроз и на-

рушений безопасности информации, с целью реализации предупреждающих и профилактических мер предотвращения угроз и нарушений безопасности информации.

5.6 Требования к защите данных мониторинга

5.6.1 В рамках мероприятий по мониторингу ИБ обеспечивают защиту получаемых, хранимых, обрабатываемых и передаваемых данных мониторинга от несанкционированного воздействия.

5.6.2 Для защиты данных мониторинга реализуют следующие меры ЗИ:

- идентификация и аутентификация пользователей при осуществлении доступа к программным и аппаратным компонентам, применяемым для мониторинга ИБ;
- управление идентификаторами пользователей при осуществлении доступа к программным и аппаратным компонентам, применяемым для мониторинга ИБ;
- управление средствами аутентификации (аутентификационной информацией) пользователей при осуществлении доступа к данным мониторинга и (или) автоматизированным средствам мониторинга;
- управление учетными записями пользователей, используемыми при осуществлении доступа к данным мониторинга и (или) автоматизированным средствам мониторинга;
- защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий (при осуществлении доступа к данным мониторинга и (или) автоматизированным средствам мониторинга);
- управление доступом пользователей при осуществлении доступа к данным мониторинга и (или) автоматизированным средствам мониторинга;
- ограничение неуспешных попыток доступа к программным и аппаратным компонентам, применяемым для доступа к данным мониторинга и (или) автоматизированным средствам мониторинга;
- регистрация действий пользователей при осуществлении доступа к данным мониторинга и (или) автоматизированным средствам мониторинга.

Примечание — В процессе мониторинга ИБ, как минимум, регистрируются следующие типы событий безопасности, связанные с доступом к данным мониторинга и (или) автоматизированным средствам мониторинга, которые установлены в ГОСТ Р 59548:

- попытки идентификации и аутентификации субъекта доступа;
- управление учетными записями пользователей;
- управление средствами аутентификации;
- управление атрибутами доступа;
- попытки доступа к защищаемой информации;
- управление (администрирование) функциями безопасности;
- действия по управлению журналами (записями) регистрации событий безопасности;
- защита от несанкционированного изменения данных аудита программных и аппаратных компонентов, применяемых для мониторинга ИБ.

Примечание — Под аудитом программных и аппаратных компонентов, применяемых для мониторинга ИБ, понимают проверку соответствия данных программных и аппаратных компонентов определенным для них инструкциям, стандартам, руководящим документам, планам и процедурам;

- оповещение оператора мониторинга ИБ о потенциально опасных действиях пользователей, осуществляющих доступ к программным и аппаратным компонентам, применяемым для доступа к данным мониторинга и (или) автоматизированным средствам мониторинга.

5.6.3 Защиту данных мониторинга ИБ осуществляют исходя из классов защищенности (категорий значимости, уровней защищенности информации) информационных (автоматизированных) систем, для которых планируется осуществлять мониторинг ИБ.

5.6.4 Применение методов криптографической защиты информации определяют в соответствии с законодательством Российской Федерации.

УДК 004.622:006.354 ОКС 35.020

Ключевые слова: мониторинг информационной безопасности, уровни, события безопасности, источники, контроль, данные

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 29.07.2021. Подписано в печать 02.08.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «РСТ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва. Нахимовский пр-т. д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru

gost.e-ecolog.ru