**Лекция 7 - 8**

**МОНИТОРИНГ ИБ**

**(**ГОСТ Р 59547-2021. Дата введения 2022-04-01**)**

**Мониторинг ИБ** – процесс постоянного наблюдения за ИС и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей.

В процессе мониторинга осуществляются:

- анализ событий безопасности и иных данных мониторинга;

- контроль (анализ) защищенности информации;

- анализ и оценка функционирования систем защиты информации (ЗИ) информационных (автоматизированных) систем;

- периодический анализ изменения угроз безопасности информации в информационных (автоматизированных) системах, возникающих в ходе эксплуатации.

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.

**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.

**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.

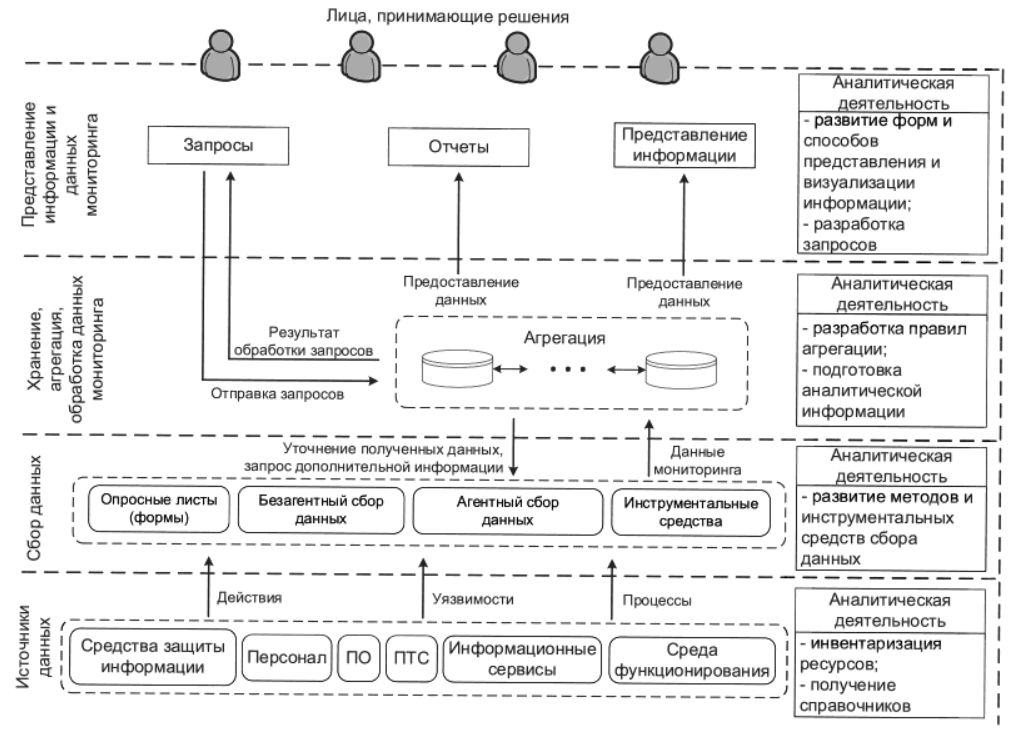


Рис. 1 Уровни мониторинга ИБ

**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.

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).

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

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

**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.

**Требования к мониторингу информационной безопасности**

– *требования к источникам данных* (данные мониторинга могут быть собраны с использованием как автоматизированных, так и неавтоматизированных средств;

– *требования к сбору данных* (осуществляют сбор исходных данных в объеме, необходимом и достаточном для проведения анализа и различного рода оценок состояния ИБ);

– *требования к хранению, агрегированию и обработке данных* мониторинга (должно обеспечиваться хранение данных, собираемых от источников, и результатов их обработки);

– *требования к представлению данных* о результатах мониторинга (необходимо обеспечивать возможность представления как собранных данных о событиях безопасности и иных данных мониторинга, так и результатов выполнения определенных настоящим стандартом мероприятий мониторинга ИБ).

**Порядок осуществления мониторинга ИБ при реализации мер по ЗИ**

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.

*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.

**Требования к защите данных мониторинга**

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.

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.

- 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.

Защиту данных мониторинга ИБ осуществляют **исходя из классов защищенности** (категорий значимости, уровней защищенности информации) информационных (автоматизированных) систем, для которых планируется осуществлять мониторинг ИБ. Всего шесть классов: C1, C2, B1, B2, B3 и A1

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