

Регистрация событий
Информационной безопасности



Регистрация событий безопасности в ИС

Одним из направлений развития средств обеспечения безопасности информационных систем является создание и усовершенствование средств регистрации и анализа событий безопасности. Обычно процесс регистрации событий безопасности в ИС принято называть аудитом.

Возможности аудита существуют во многих операционных системах (ОС) и прикладном программном обеспечении (ПО). Часто подсистемы аудита обеспечивают лишь регистрацию информации о различных событиях, возможности анализа зачастую отсутствуют, а если и существуют, то очень ограниченные. Поэтому для эффективного решения задачи регистрации и анализа событий безопасности требуется специальное программное обеспечение, которое использует данные встроенных подсистем аудита операционных систем и прикладного программного обеспечения.

Определение **событий безопасности**, подлежащих регистрации, и сроков их хранения

События безопасности, подлежащие регистрации в ИСПДн, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите персональных данных в ИСПДн.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется оператором персональных данных исходя из возможностей реализации угроз безопасности персональных данных и фиксируется в организационно-распорядительных документах по защите персональных данных (документируется).

В ИСПДн как минимум подлежат регистрации следующие события:



вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;



подключение машинных носителей информации и вывод персональных данных на носители информации;



запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой персональных данных;



попытки доступа программных средств к определяемым оператором персональных данных защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;



попытки удаленного доступа.

Обязанности оператора по РСБ:

оператором должен обеспечиваться пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем **один раз в год**, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;



оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с действиями **от имени** привилегированных учетных записей (администраторов);




оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с **изменением привилегий** учетных записей;



оператором должен быть обеспечен срок хранения информации о зарегистрированных событиях безопасности не менее **трех месяцев**, если иное не установлено требованиями законодательства Российской Федерации.



РЕАГИРОВАНИЕ НА СБОИ



В информационной системе персональных данных должно осуществляться реагирование на сбои при регистрации событий безопасности, **в том числе** аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема памяти.

Реагирование на сбои при регистрации **обязано предусматривать:**

- предупреждение администраторов при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности



-[Понятие инцидента]-

ИНЦИДЕНТ

Согласно международным регламентам, инцидентом информационной безопасности является **единичное событие** нежелательного и непредсказуемого характера, которое способно **повлиять** на бизнес-процессы компании, скомпрометировать их или нарушить степень защиты информационной безопасности.



На практике к этому понятию относятся **разноплановые события**, происходящие в процессе работы с информацией, существующей в электронной форме или на материальных носителях. К ним может относиться и **оставление документов** на рабочем столе в свободном доступе для другого персонала, и хакерская атака – оба инцидента в равной мере могут нанести **ущерб** интересам компании.

-[ВСЕ ПРО СОБЫТИЯ]-

Типы событий

Все эти события должны быть классифицированы, описаны и внесены во внутренние документы компании, регламентирующие порядок обеспечения информационной безопасности.

нарушение порядка взаимодействия с Интернет-провайдерами, хостингами, почтовыми сервисами, облачными сервисами и другими поставщиками телекоммуникационных услуг;

отказ оборудования по любым причинам, как технического, так и программного характера;

нарушение работы программного обеспечения;

нарушение любых правил обработки, хранения, передачи информации, как электронной, так и документов;

выявление внешнего мониторинга ресурсов;

выявление вирусов или других вредоносных программ;

неавторизированный или несанкционированный доступ третьих лиц к информационным ресурсам;

любая компрометация системы, например, попадание пароля от учетной записи в открытый доступ.

- [ЖУРНАЛ СОБЫТИЙ] -



Начат: _____

Окончен: _____

№ п/п	Дата события	Основания возникновения события	Описание события (мероприятия)	Характеристика события	(ФИО, субъекта)	Должность, ФИО и подпись ответственного за ведение журнала	Примечание

Журнал событий

События информационной безопасности фиксируются документально в журнале учета событий информации.

Основные этапы создания СМИБ



Процесс внедрения любой системы мониторинга событий информационной безопасности включает в себя следующие основные этапы:

- **обследование** автоматизированной системы. В рамках обследования проводится идентификация основных источников событий безопасности, определение технологии сбора, хранения и обработки данных. По результатам обследования формируются **требования** к архитектуре и функциональным возможностям системы мониторинга информационной безопасности;

-[СМИБ]-

Основные этапы создания СМИБ



Процесс внедрения любой системы мониторинга событий информационной безопасности включает в себя следующие основные этапы:

- разработка технического проекта, в котором **описывается** конфигурация оборудования и программного обеспечения, порядок внедрения, схема информационных потоков, требования к внешнему окружению системы мониторинга и т.д.;

-[СМИБ]-

Основные этапы создания СМИБ



Процесс внедрения любой системы мониторинга событий информационной безопасности включает в себя следующие основные этапы:

- обучение **сотрудников**, которые будут отвечать за эксплуатацию системы мониторинга информационной безопасности;

Основные этапы создания СМИБ



Процесс внедрения любой системы мониторинга событий информационной безопасности включает в себя следующие основные этапы:

- создание пилотного района для тестового внедрения системы **мониторинга** информационной безопасности. Если объектом мониторинга является территориально-распределённая система, охватывающая несколько филиалов, то в качестве тестового сегмента, как правило, выбирается **наиболее крупное** подразделение, на котором можно апробировать решения, описанные в техническом проекте.

-[СМИБ]-

Основные этапы создания СМИБ



Процесс внедрения любой системы мониторинга событий информационной безопасности включает в себя следующие основные этапы:

- промышленное внедрение системы мониторинга. Внедрение проводится с учетом результатов, полученных в процессе тестового внедрения системы мониторинга;

-[СМИБ]-

Основные этапы создания СМИБ



Процесс внедрения любой системы мониторинга событий информационной безопасности включает в себя следующие основные этапы:

- техническое **сопровождение** системы мониторинга информационной безопасности.

-[СПАСИБО!]-

ИСТОЧНИКИ

- <https://fstec21.blogspot.com/2017/07/the-definition-of-security-events-to-be.html>
- <https://bazanpa.ru/fstek-rossii-metodika-ot11022014-h2252143/3/3.5/3.5.1/>
- <https://cyberleninka.ru/article/n/registratsiya-i-analiz-sobytiy-bezopasnosti-v-informatsionnyh-sistemah>
- <https://www.securitylab.ru/blog/personal/sborisov/120692.php>