УТВЕРЖДЕНЫ
приказом ФСТЭК России
от « 14 » апреля 2023 г. № 64

Требования по безопасности информации к системам управления базами данных (выписка)

1. Настоящие Требования являются обязательными требованиями в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа[1] (далее – требования по безопасности информации), предъявляемыми к программным средствам, реализующим функциональные возможности по созданию баз данных, манипулированию данными (вставке, обновлению, удалению, выборке), обеспечению безопасности, надежности хранения и целостности данных, администрированию баз данных, а также обеспечивающим управление доступом субъектов доступа к объектам доступа баз данных, предназначенных для хранения информации, подлежащей защите в информационной (автоматизированной) системе (далее – системы управления базами данных).

2. Выполнение настоящих Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической защиты информации и средств обеспечения безопасности информационных технологий, организуемых ФСТЭК России в пределах своих полномочий в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55 (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063) (с изменениями, внесенными приказом ФСТЭК России от 5 августа 2021 г. № 121 (зарегистрирован Минюстом России 27 октября 2021 г., регистрационный № 65594) и приказом ФСТЭК России от 19 сентября 2022 г. № 172 (зарегистрирован Минюстом России 19 октября 2022 г., регистрационный № 70614).

3. К системам управления базами данных устанавливается 6 классов защиты.

---

1 Статья 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

Системы управления базами данных, соответствующие 6 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 3 категории значимости[2], в государственных информационных системах 3 класса защищенности[3], в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности[4], в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных[5].

Системы управления базами данных соответствующие 5 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 2 категории значимости, в государственных информационных системах 2 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных.

Системы управления базами данных, соответствующие 4 классу защиты, применяются в значимых объектах критической информационной инфраструктуры 1 категории значимости, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса[6].

4. Настоящие Требования включают требования по безопасности информации, предъявляемые к:

уровню доверия системы управления базами данных;

операционной системе, в среде которой функционирует система управления базами данных;

управлению доступом в системе управления базами данных;

---

2 Статья 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

3 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933), приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924) и приказом ФСТЭК России от 27 апреля 2020 г. № 61 (зарегистрирован Минюстом России 12 мая 2020 г., регистрационный № 58322).

4 Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 32919) (с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487), приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071) и приказом ФСТЭК России от 15 марта 2021 г. № 46 (зарегистрирован Минюстом России 1 июля 2021 г., регистрационный № 64063).

5 Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

6 Требования о защите информации, содержащейся в информационных системах общего пользования, утвержденные приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 (зарегистрирован Минюстом России 13 октября 2010 г., регистрационный № 18704).

идентификации и аутентификации пользователей в системе управления базами данных;

контролю целостности в системе управления базами данных;

регистрации событий безопасности в системе управления базами данных;

резервному копированию и восстановлению в системе управления базами данных;

обеспечению доступности системы управления базами данных;

очистке памяти в системе управления базами данных;

производительности системы управления базами данных;

ограничению программной среды в системе управления базами данных.

5. Система управления базами данных должна соответствовать Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59772) (с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 г. № 68 (зарегистрирован Минюстом России 20 июля 2022 г., регистрационный № 69318).

Устанавливается следующее соответствие классов защиты систем управления базами данных уровням доверия:

системы управления базами данных 6 класса защиты должны соответствовать 6 уровню доверия;

системы управления базами данных 5 класса защиты должны соответствовать 5 уровню доверия;

системы управления базами данных 4 класса защиты должны соответствовать 4 уровню доверия;

6. Операционная система, в среде которой функционирует система управления базами данных, должна быть сертифицирована на соответствие Требованиям в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требованиям безопасности информации к операционным системам), утвержденным приказом ФСТЭК России от 19 августа 2016 г. № 119 (зарегистрирован Минюстом России 19 сентября 2016 г., регистрационный № 43691), и Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76.

Система управления базами данных должна функционировать в среде сертифицированной операционной системы, имеющей класс защиты не ниже класса защиты системы управления базами данных.

7. К управлению доступом в системе управления базами данных предъявляются следующие требования:

7.1. В системе управления базами данных 6, 5, 4 классов защиты должны быть реализованы дискреционный и ролевой методы управления доступом.

Ролевой метод управления доступом должен быть реализован для следующих ролей пользователей системы управления базами данных: администратор системы управления базами данных, администратор базы данных (администратор информационной системы), пользователь базы данных (пользователь информационной системы).

Система управления базами данных 6, 5, 4 классов защиты должна обеспечивать наделение администратора системы управления базами данных следующими правами:

создавать учетные записи пользователей системы управления базами данных;

модифицировать, блокировать и удалять учетные записи пользователей системы управления базами данных;

назначать права доступа пользователям системы управления базами данных к объектам доступа системы управления базами данных;

управлять конфигурацией системы управления базами данных;

создавать, подключать базы данных.

Система управления базами данных 6, 5, 4 классов защиты должна обеспечивать наделение администратора базы данных (администратора информационной системы) следующими правами:

создавать учетные записи пользователей базы данных;

модифицировать, блокировать и удалять учетные записи пользователей базы данных;

управлять конфигурацией базы данных;

назначать права доступа пользователям базы данных (пользователей информационной системы) к объектам доступа базы данных;

создавать резервные копии базы данных и восстанавливать базу данных из резервной копии;

создавать, модифицировать и удалять процедуры (программный код), хранимые в базе данных.

Система управления базами данных 6, 5, 4 классов защиты должна обеспечивать наделение пользователя базы данных (пользователя информационной системы) следующими правами:

создавать и манипулировать объектами доступа базы данных (таблица, запись или столбец, поле, представление и иные объекты доступа);

выполнять процедуры (программный код), хранимые в базе данных.

Дискреционный метод управления доступом субъектов доступа к объектам доступа системы управления базами данных (база данных, таблица, запись или столбец, поле, представление, процедура (программный код) или иные объекты доступа) должен осуществляться на основе настраиваемых списков управления доступом (матриц управления доступом).

Списки управления доступом (матрицы управления доступом) должны позволять задавать разрешение или запрет пользователям системы управления базами данных выполнять следующие операции в отношении процедур (программного кода), хранимых в базе данных: создание; модификация, удаление, исполнение.

Списки управления доступом (матрицы управления доступом) должны позволять задавать разрешение или запрет пользователям и процедурам (программному коду), хранимым в базе данных, выполнять следующие операции в отношении объектов доступа системы управления базами данных (база данных, таблица, запись или столбец, поле, представление или иные объекты доступа): создание, модификация, удаление, чтение.

8. К идентификации и аутентификации пользователей в системе управления базами данных предъявляются следующие требования:

8.1. Первичная идентификация администраторов системы управления базами данных и администраторов баз данных (администраторов информационных систем) 6 класса защиты должна осуществляться администратором системы управления базами данных.

Первичная идентификация пользователей базы данных должна осуществляться администратором базы данных (администратором информационной системы).

Идентификация и аутентификация пользователей в системе управления базами данных осуществляется с учетом требований разделов 4-7 ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения»[7].

Система управления базами данных должна осуществлять аутентификацию пользователей системы управления базами данных при предъявлении пароля пользователя.

Пароль пользователя для администраторов системы управления базами данных и администраторов базы данных (администратором информационной

---

7 Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 10 апреля 2020 г. № 159-ст (М., «Стандартинформ», 2020).

системы) должен устанавливаться администратором системы управления базами данных. Пароль для пользователей базы данных устанавливается администратором базы данных (администратором информационной системы).

Система управления базами данных должна обеспечивать возможность смены установленных паролей пользователей системы управления базами данных после их первичной аутентификации.

При попытке ввода неправильного значения идентификатора или пароля пользователя системы управления базами данных должно быть отказано в доступе.

При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись пользователя базы данных (пользователя информационной системы) должна быть заблокирована системой управления базами данных с возможностью разблокировки администратором системы управления базами данных или администратором базы данных (администратором информационной системы) или с возможностью автоматической разблокировки по истечении временного интервала.

При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись администратора системы управления базами данных или администратора базы данных (администратора информационной системы) должна быть заблокирована системой управления базами данных с возможностью разблокировки администратором системы управления базами данных или с возможностью автоматической разблокировки по истечении временного интервала.

Защита пароля пользователя системы управления базами данных должна обеспечиваться при его вводе за счет исключения отображения символов вводимого пароля или отображения вводимых символов условными знаками.

Пароль пользователя системы управления базами данных 6 класса защиты должен содержать не менее 6 символов при алфавите пароля не менее 60 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 10.

Система управления базами данных должна обеспечивать хранение аутентификационной информации пользователя системы управления базами данных в защищенном формате или в защищенном хранилище.

8.2. Пароль пользователя системы управления базами данных 5 класса защиты должен содержать не менее 6 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 8.

8.3. Пароль пользователя системы управления базами данных 4 класса защиты должен содержать не менее 8 символов при алфавите пароля не менее

70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 4.

9. К контролю целостности в системе управления базами данных предъявляются следующие требования:

9.1. Система управления базами данных 6, 5 класса защиты должна:

контролировать целостность конфигурации системы управления базами данных, конфигураций баз данных, процедур (программного кода) системы управления базами данных, процедур (программного кода), хранимых в базах данных, в процессе запуска системы управления базами данных самостоятельно или с применением сертифицированной операционной системы;

информировать администратора системы управления базами данных о нарушении целостности объектов контроля;

информировать администратора базы данных (администратора информационной системы) о нарушении целостности конфигураций баз данных, процедур (программного кода), хранимых в базах данных;

блокировать доступ пользователей системы управления базами данных (за исключением администратора системы управления базами данных) к системе управления базами данных и базам данных при выявлении нарушения целостности объектов контроля;

блокировать доступ пользователей базы данных (пользователей информационной системы) к базе данных при выявлении нарушения целостности конфигураций баз данных, процедур (программного кода), хранимых в базах данных.

9.2. Система управления базами данных 4 класса защиты наряду с требованиями, установленными подпунктом 9.1 пункта 9 настоящих Требований, дополнительно должно контролировать целостность процедур (программного кода) системы управления базами данных, процедур (программного кода), хранимых в базах данных, в процессе функционирования системы управления базами данных не реже одного раза в сутки.

10. К регистрации событий безопасности в системе управления базами данных предъявляются следующие требования:

10.1. Система управления базами данных 6, 5 классов защиты должна:

обеспечивать регистрацию событий безопасности, связанных с функционированием системы управления базами данных и действиями пользователей системы управления базами данных;

оповещать администратора системы управления базами данных, администратора базы данных (администратора информационной системы) о событиях безопасности;

осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие события происходили.

Регистрация событий безопасности в системе управления базами данных должна осуществляться с учетом требований разделов 5-6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации»[8].

Для каждой функции безопасности в системе управления базами данных должен быть определен перечень событий, необходимых для регистрации и учета.

Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться номер (уникальный идентификатор) события, дата, время, тип события безопасности.

Записи журнала событий безопасности должны представляться в структурированном виде и содержать дату и время события безопасности, взятое из аппаратной платформы или операционной системы.

Журнал событий безопасности системы управления базами данных должен быть доступен для чтения администратору системы управления базами данных и администратору базы данных. Для пользователя базы данных (пользователя информационной системы) журнал событий безопасности системы управления базами данных должен быть недоступен. При исчерпании области памяти, отведенной под журнал событий безопасности системы управления базами данных, система управления базами данных должна осуществлять самостоятельно или с применением механизмов сертифицированной операционной системы архивирование журнала с последующей очисткой высвобождаемой области памяти.

Регистрации подлежат как минимум следующие события безопасности:

создание учетных записей пользователей системы управления базами данных;

изменение атрибутов учетных записей пользователей системы управления базами данных;

успешные и неуспешные попытки аутентификации пользователей системы управления базами данных;

запуск и остановка системы управления базами данных с указанием причины остановки;

изменение конфигурации системы управления базами данных;

создание и удаление базы данных, таблицы за исключением временных таблиц, создаваемых системой управления базами данных в служебных целях;

---

8 Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 13 января 2022 г. № 2-ст (М., «Стандартинформ», 2022).

подключение, восстановление базы данных;

изменение правил разграничения доступа в системе управления базами данных;

факты нарушения целостности объектов контроля;

создание и изменение процедур (программного кода), хранимых в базах данных, и представлений.

10.2. В системе управления базами данных 4 класса защиты наряду с требованиями, установленными подпунктом 10.1 пункта 10 настоящих Требований, для регистрируемых событий безопасности в каждой записи журнала событий безопасности дополнительно должны регистрироваться сведения о важности события.

11. К резервному копированию и восстановлению в системе управления базами данных предъявляются следующие требования:

11.1. В системе управления базами данных 6, 5 классов защиты должно обеспечиваться резервное копирование и восстановление баз данных и их конфигураций, в том числе атрибутов безопасности, самостоятельно или с применением сертифицированных операционной системы или средства резервного копирования.

11.2. В системе управления базами данных 4 класса защиты наряду с требованиями, установленными подпунктом 11.1 пункта 11 настоящих Требований, дополнительно должно обеспечиваться резервное копирование конфигурации системы управления базами данных самостоятельно или с применением сертифицированных операционной системы или средства резервного копирования.

12. К обеспечению доступности в системе управления базами данных предъявляются следующие требования:

система управления базами данных 4 класса защиты должна функционировать в отказоустойчивом кластере, обеспечивающем её доступность, за счет одновременного функционирования нескольких экземпляров системы управления базами данных;

система управления базами данных должна обеспечивать возможность синхронизации параметров конфигурации систем управления базами данных в кластере;

в формуляре системы управления базами данных должны быть приведены параметры конфигурации кластера систем управления базами данных, позволяющие обеспечить обработку отказов заданного количества узлов кластера;

должна обеспечиваться возможность поочередного обновления, связанного с устранением уязвимостей, каждой системы управления базами

данных или компонентов в кластере при сохранении доступности системы управления базами данных.

при неуспешном обновлении системы управления базами данных в кластере должна обеспечиваться возможность возврата к её предыдущему состоянию. Данное действие не должно приводить к прерыванию работы кластера систем управления базами данных.

13. К очистке памяти в системе управления базами данных предъявляются следующие требования:

13.1. Система управления базами данных 6, 5 классов защиты самостоятельно или с применением сертифицированной операционной системы должна обеспечивать удаление баз данных и журналов, используемых системой управления базами данных, путем многократной перезаписи уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями.

13.2. Система управления базами данных 4 класса защиты наряду с требованиями, установленными подпунктом 13.1 пункта 13 настоящих Требований, дополнительно должна удалять объекты доступа базы данных, используемые системой управления базами данных, путем перезаписи модифицированных участков объектов файловой системы при выполнении операции удаления или в отложенном режиме через промежуток времени, устанавливаемый администратором системы управления базами данных или администратором базы данных.

14. Система управления базами данных 6, 5, 4 классов защиты должна обеспечивать производительность со следующими параметрами:

количество пользовательских сессий, поддерживаемых параллельно;

количество обрабатываемых стандартных запросов в единицу времени;

количество транзакций в единицу времени;

задержка в выполнении стандартного запроса, определенного в документации системы управления базами данных;

количество экземпляров системы управления базами данных, которые могут совместно работать в режиме балансировки нагрузки.

Сведения о значениях данных параметров производительности в зависимости от параметров настройки системы управления базы данных и условий функционирования системы управления базами данных должны быть приведены в формуляре системы управления базами данных.

15. К ограничению программной среды в системе управления базами данных предъявляются следующие требования:

15.1. Система управления базами данных 6, 5 классов защиты самостоятельно или с привлечением сертифицированной операционной

системы должна выявлять и блокировать загрузку в адресное пространство системы управления базами данных программного обеспечения, не включенного в перечень (список) программного обеспечения, разрешенного для выполнения.

15.2. Система управления базами данных 4 класса защиты наряду с требованиями, установленными подпунктом 15.1 пункта 15 настоящих Требований, дополнительно должна:

запрещать создание процедур (программного кода), хранимых в базах данных, пользователям баз данных (пользователям информационной системы);

размещать код системы управления базами данных в области памяти, не доступной одновременно для записи и исполнения;

выявлять и блокировать загрузку в адресное пространство системы управления базами данных программного обеспечения, целостность которого нарушена.