**МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ МАОУ СОШ № 6**

**«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 6»**

|  |
| --- |
| ИНН 6625017376 КПП 662501001 623114, Свердловская область, город Первоуральск, проспект Космонавтов 12тел./факс (3439) 64-17-08, 64-87-60 E-mail: mаouschool\_6@mail.ru  |

**ПРИКАЗ**

15.08.2025 № 01-11 / 331

г. Первоуральск

***Об обеспечении безопасности персональных данных при их обработке в***

***Муниципальном автономном общеобразовательном***

***учреждении «Средняя общеобразовательная школа № 6»***

***(МАОУ СОШ № 6)***

В целях выполнения обязанностей оператора, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МАОУ СОШ № 6, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных, а также обеспечения защиты информации в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

ПРИКАЗЫВАЮ:

1. Утвердить инструкции при реализации организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МАОУ СОШ № 6, необходимых для обеспечения 4 уровня защищенности персональных данных, в соответствии с составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённым приказом ФСТЭК России от 18.02.2013 №21:
	1. инструкции по идентификации и аутентификация субъектов доступа и объектов доступа:
		1. инструкция по идентификации и аутентификация пользователей, являющихся работниками оператора – приложение 1 настоящего приказа;
		2. инструкция по управлению идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов – приложение 2 настоящего приказа;
		3. инструкция по управлению средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации – приложение 3 настоящего приказа;
		4. инструкция по защите обратной связи при вводе аутентификационной информации – приложение 4 настоящего приказа;
		5. инструкция по идентификации и аутентификации пользователей, не являющихся работниками оператора (внешних пользователей) – приложение 5 настоящего приказа.
	2. инструкции по управлению доступом субъектов доступа к объектам доступа:
		1. инструкция по управлению (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей – приложение 6 настоящего приказа;
		2. инструкция по реализации необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа – приложение 7 настоящего приказа;
		3. инструкция по управлению (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами – приложение 8 настоящего приказа;
		4. инструкция по разделению полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы - приложение 9 настоящего приказа;
		5. инструкция по назначению минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы – приложение 10 настоящего приказа;
		6. инструкция по ограничению неуспешных попыток входа в информационную систему (доступа к информационной системе) – приложение 11 настоящего приказа;
		7. инструкция по реализации защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети – приложение 12 настоящего приказа;
		8. инструкция по регламентации и контролю использования в информационной системе технологий беспроводного доступа – приложение 13 настоящего приказа;
		9. инструкция по регламентации и контролю использования в информационной системе мобильных технических средств – приложение 14 настоящего приказа;
		10. инструкция по управлению взаимодействием с информационными системами сторонних организаций (внешние информационные системы) – приложение 15 настоящего приказа.
	3. инструкции по регистрации событий безопасности:
		1. инструкция по определению событий безопасности, подлежащих регистрации, и сроков их хранения – приложение 16 настоящего приказа;
		2. инструкция по определению состава и содержания информации о событиях безопасности, подлежащих регистрации – приложение 17 настоящего приказа;
		3. инструкция по сбору, записи и хранению информации о событиях безопасности в течение установленного времени хранения - приложение 18 настоящего приказа;
		4. инструкция по защите информации о событиях безопасности – приложение 19 настоящего приказа.
	4. инструкции по организации антивирусной защиты:
		1. инструкция по реализации антивирусной защиты - приложение 20 настоящего приказа;
		2. инструкция по обновлению базы данных признаков вредоносных компьютерных программ (вирусов) – приложение 21 настоящего приказа.
	5. инструкции по контролю (анализу) защищенности персональных данных (АНЗ):
		1. инструкция по контролю установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации – приложение 22 настоящего приказа.
	6. инструкции по защите среды виртуализации:
		1. инструкция по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации – приложение 23 настоящего приказа;
		2. инструкция по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин – приложение 24 настоящего приказа.
	7. инструкции по защите технический средств:
		1. инструкция по контролю и управлению физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены – приложение 25 настоящего приказа;
		2. инструкция по размещению устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр – приложение 26 настоящего приказа.
	8. инструкции по защите информационной системы, ее средств, систем связи и передачи данных:
		1. инструкция по обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи – приложение 27 настоящего приказа.
2. Утвердить инструкции при реализации организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МАОУ СОШ № 6, необходимых для обеспечения 3 уровня защищенности персональных данных, в соответствии с составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённым приказом ФСТЭК России от 18.02.2013 №21:
	1. инструкции по управлению доступом субъектов доступа к объектам доступа:
		1. инструкция по блокированию сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу – приложение 28 настоящего приказа;
		2. инструкция по разрешению (запрету) действий пользователей, разрешенных до идентификации и аутентификации – приложение 29 настоящего приказа;
		3. инструкция по уничтожению (стиранию) или обезличиванию персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контролю уничтожения (стирания) или обезличивания – приложение 30 настоящего приказа.
	2. инструкции по контролю (анализу) защищенности персональных данных:
		1. инструкция по выявлению, анализу уязвимостей информационной системы и оперативному устранению вновь выявленных уязвимостей – приложение 31 настоящего приказа;
		2. инструкция по контролю работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации – приложение 32 настоящего приказа;
		3. инструкция по контролю состава технических средств, программного обеспечения и средств защиты информации – приложение 33 настоящего приказа.
	3. инструкции по защите среды виртуализации:
		1. инструкция по регистрации событий безопасности в виртуальной инфраструктуре – приложение 34 настоящего приказа;
		2. инструкция по реализации и управлению антивирусной защитой в виртуальной инфраструктуре – приложение 35 настоящего приказа;
		3. инструкция по разбиению виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей – приложение 36 настоящего приказа;
	4. инструкции по защите информационной системы, ее средств, систем связи и передачи данных:
		1. инструкция по защите беспроводных соединений, применяемых в информационной системе – приложение 37 настоящего приказа.
	5. инструкции по управлению конфигурацией информационной системы и системы защиты персональных данных – приложение 38 настоящего приказа.
3. Утвердить инструкции при реализации организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МАОУ СОШ № 6, необходимых для обеспечения 2 уровня защищенности персональных данных, в соответствии с составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённым приказом ФСТЭК России от 18.02.2013 №21:
	1. инструкции по идентификации и аутентификация субъектов доступа и объектов доступа:
		1. инструкция по идентификации и аутентификации устройств, в том числе стационарных, мобильных и портативных – приложение 39 настоящего приказа.
	2. инструкции по управлению доступом субъектов доступа к объектам доступа:
		1. инструкция по обеспечению доверенной загрузки средств вычислительной техники – приложение 40 настоящего приказа.
	3. инструкции по ограничению программной среды:
		1. инструкция по управлению установкой (инсталляцией) компонентов программного обеспечения, в том числе определению компонентов, подлежащих установке, настройке параметров установки компонентов, контролю за установкой компонентов программного обеспечения – приложение 41 настоящего приказа.
	4. инструкции по защите машинных носителей персональных данных:
		1. инструкция по учету машинных носителей персональных данных – приложение 42 настоящего приказа;
		2. инструкция по управлению доступом к машинным носителям персональных данных – приложение 43 настоящего приказа.
	5. инструкции по регистрации событий безопасности:
		1. инструкция по мониторингу (просмотр, анализ) результатов регистрации событий безопасности и реагированию на них – приложение 44 настоящего приказа.
	6. инструкции по обнаружению вторжений:
		1. инструкция по обнаружению вторжений – приложение 45 настоящего приказа;
		2. инструкция по обновлению базы решающих правил – приложение 46 настоящего приказа.
	7. инструкции по контролю (анализу) защищенности персональных данных:
		1. инструкция по контролю правил генерации и смены паролей пользователей, заведения и удалению учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе – приложение 47 настоящего приказа.
	8. инструкции по обеспечению целостности информационной системы и персональных данных:
		1. инструкция по контролю целостности программного обеспечения, включая программное обеспечение средств защиты информации – приложение 48 настоящего приказа;
		2. инструкция по обнаружению и реагированию на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) – приложение 49 настоящего приказа.
	9. инструкции по обеспечению доступности персональных данных:
		1. инструкция по периодическому резервному копированию персональных данных на резервные машинные носители персональных данных – приложение 50 настоящего приказа;
		2. инструкция по обеспечению возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала – приложение 51 настоящего приказа.
	10. инструкции по защите среды виртуализации:
		1. инструкция по управлению перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных – приложение 52 настоящего приказа;
		2. инструкция по контролю целостности виртуальной инфраструктуры и ее конфигураций – приложение 53 настоящего приказа;
		3. инструкция по резервному копированию данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры – приложение 54 настоящего приказа.
	11. инструкции по защите информационной системы, ее средств, систем связи и передачи данных:
		1. инструкция по обеспечению подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов – приложение 55 настоящего приказа;
		2. инструкция по защите архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных – приложение 56 настоящего приказа;
		3. инструкция по разбиению информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы – приложение 57 настоящего приказа.
	12. инструкции по выявлению инцидентов и реагированию на них – приложение 58 настоящего приказа.

Приложение: на 84 л. в 1 экз.

Директор школы О.В. Ошуркова

Приложение 1

к приказу

от15.08.2025 №01-11/331

Инструкция

по идентификации и аутентификации пользователей,

являющихся работниками оператора

1. В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.
2. При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.
3. К внутренним пользователям в целях настоящего документа, относятся должностные лица оператора (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств информационной системы в соответствии с должностными регламентами (инструкциями) утвержденными оператором и которым в информационной системе присвоены учетные записи.
4. В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами оператора и которым в информационной системе также присвоены учетные записи.
5. Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации УПД.11 (приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказа 21).
6. Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации – определенной комбинации указанных средств.
7. В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.
8. Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах по защите информации.

Приложение 2

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

Оператором должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в информационной системе:

1. определение должностного лица (администратора) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;
2. формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
3. присвоение идентификатора пользователю и (или) устройству;
4. предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени;
5. блокирование идентификатора пользователя после установленного оператором времени неиспользования.

Правила и процедуры управления идентификаторами регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 3

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению средствами аутентификации, в том числе хранению, выдаче, инициализации, блокировании средств аутентификации и принятию мер в случае утраты и (или) компрометации средств аутентификации

Оператором должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе:

1. определение должностного лица (администратора) оператора, ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
2. изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;
3. выдача средств аутентификации пользователям;
4. генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
5. установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля):
	1. задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;
	2. задание минимального количества измененных символов при создании новых паролей;
	3. задание максимального времени действия пароля;
	4. задание минимального времени действия пароля
	5. запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей.
6. блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;
7. назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);
8. обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором;
9. защита аутентификационной информации от неправомерного доступа к ней и модифицирования.

Правила и процедуры управления средствами аутентификации (аутентификационной информацией) регламентируются в организационно распорядительных документах оператора по защите информации.

Приложение 4

к приказу

от15.08.2025 №01-11/331

Инструкция

по защите обратной связи при вводе аутентификационной информации

В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «\*», «» или иными знаками.

Приложение 5

к приказу

от15.08.2025 №01-11/331

Инструкция

по идентификации и аутентификации пользователей, не являющихся работниками оператора (внешних пользователей)

В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей.

К пользователям, не являющимся работникам оператора (внешним пользователям), относятся все пользователи информационной системы, не указанные в ИАФ.1 (Приказа 21) в качестве внутренних пользователей. Примером внешних пользователей являются граждане, на законных основаниях через сеть Интернет получающие доступ к информационным ресурсам портала Государственных услуг Российской Федерации «Электронного правительства» или официальным сайтам в сети Интернет органов государственной власти.

Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации УПД.11 (Приказа 21).

Идентификация и аутентификация внешних пользователей в целях предоставления государственных услуг осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977.

Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 6

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

Оператором должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

1. определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);
2. объединение учетных записей в группы (при необходимости);
3. верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
4. заведение, активация, блокирование и уничтожение учетных записей пользователей;
5. пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором;
6. порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;
7. оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
8. уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;
9. предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

Правила и процедуры управления учетными записями пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 7

к приказу

от15.08.2025 №01-11/331

Инструкция

по реализации необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

Методы управления доступом реализуются в зависимости от особенностей функционирования информационной системы, с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов:

1. дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;
2. ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);
3. мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа.

Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

Правила разграничения доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 8

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

1. фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором;
2. разрешение передачи информации в информационной системе только по маршруту, установленному оператором;
3. изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором;
4. запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором.

Управление информационными потоками должно обеспечивать разрешенный (установленный оператором) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет(или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

Правила и процедуры управления информационными потоками регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 9

к приказу

от15.08.2025 №01-11/331

Инструкция

по разделению полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

Оператором должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с УПД.2 (Приказа 21).

Приложение 10

к приказу

от15.08.2025 №01-11/331

Инструкция

по назначению минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

Оператором должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

Оператором должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий. Доступ к объектам доступа с учетом минимально необходимых прав и привилегий обеспечивается в соответствии с УПД.2 (Приказа 21).

Приложение 11

к приказу

от15.08.2025 №01-11/331

Инструкция

по ограничению неуспешных попыток входа в информационную систему (доступа к информационной системе)

В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе).

Ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) должно обеспечиваться в соответствии с ИАФ.4 (Приказа 21).

Приложение 12

к приказу

от15.08.2025 №01-11/331

Инструкция

по реализации защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает:

1. установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы;
2. ограничение на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с УПД.2 (Приказа 21);
3. предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
4. мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы;
5. контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации).

Правила и процедуры применения удаленного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 13

к приказу

от15.08.2025 №01-11/331

Инструкция

по регламентации и контролю использования в информационной системе технологий беспроводного доступа

Оператором должны обеспечиваться регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе.

Регламентация и контроль использования технологий беспроводного доступа должны включать:

1. ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление беспроводного доступа в соответствии с УПД.2 (Приказа 21);
2. предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
3. мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной системы;
4. контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой.

Правила и процедуры применения технологий беспроводного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 14

к приказу

от15.08.2025 №01-11/331

Инструкция

по регламентации и контролю использования в информационной системе мобильных технических средств

Оператором должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе.

В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

Регламентация и контроль использования мобильных технических средств должны включать:

1. установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа информационной системы с использованием мобильных технических средств, входящих в состав информационной системы;
2. использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с ЗИС.30 (Приказа 21);
3. ограничение на использование мобильных технических средств в соответствии с задачами (функциями) информационной системы, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с УПД.2 (Приказа 21);
4. мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы;
5. запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством.

Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 15

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

Оператором должно быть обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности) уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования информационной системы.

Управление взаимодействием с внешними информационными системами должно включать:

1. предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям в соответствии с УПД.2 (Приказа 21);
2. определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;
3. определение системных учетных записей, используемых в рамках данного взаимодействия;
4. определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;
5. определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

Управление взаимодействием с внешними информационными системами в целях межведомственного электронного взаимодействия, исполнения государственных и муниципальных функций, формирования базовых государственных информационных ресурсов осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977.

Правила и процедуры управления взаимодействием с внешними информационными системами регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 16

к приказу

от15.08.2025 №01-11/331

Инструкция

по определению событий безопасности, подлежащих регистрации,

и сроков их хранения

Оператором должны быть определены события безопасности в информационной системе, подлежащие регистрации, и сроки их хранения.

События безопасности, подлежащие регистрации в информационной системе, должны определяться с учетом способов реализации угроз безопасности для информационной системы. К событиям безопасности, подлежащим регистрации в информационной системе, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации.

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

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

В информационной системе как минимум подлежат регистрации следующие события:

1. вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;
2. подключение машинных носителей информации и вывод информации на носители информации;
3. запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
4. попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
5. попытки удаленного доступа.

Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с РСБ.2 (Приказа 21).

Приложение 17

к приказу

от15.08.2025 №01-11/331

Инструкция

по определению состава и содержания информации о событиях безопасности, подлежащих регистрации

В информационной системе должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

Состав и содержание информации о событиях безопасности, подлежащих регистрации, отражаются в организационно-распорядительных документах оператора по защите информации.

Приложение 18

к приказу

от15.08.2025 №01-11/331

Инструкция

по сбору, записи и хранению информации о событиях безопасности в течение установленного времени хранения

В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности.

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

1. возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в соответствии с РСБ.1 (Приказа 21);
2. генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с РСБ.1 (Приказа 21) с составом и содержанием информации, определенными в соответствии с РСБ.2 (Приказа 21);
3. хранение информации о событиях безопасности в течение времени, установленного в соответствии с РСБ.1 (Приказа 21).

Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с РСБ.1 (Приказа 21), составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с РСБ.2 (Приказа 21), прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с РСБ.1 (Приказа 21).

Правила и процедуры сбора, записи и хранения информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 19

к приказу

от15.08.2025 №01-11/331

Инструкция

по защите информации о событиях безопасности

В информационной системе должна обеспечиваться защита информации о событиях безопасности.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с настоящим методическим документом, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

Правила и процедуры защиты информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 20

к приказу

от15.08.2025 №01-11/331

Инструкция

по реализации антивирусной защиты

Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Реализация антивирусной защиты должна предусматривать:

1. применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);
2. установку, конфигурирование и управление средствами антивирусной защиты;
3. предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;
4. проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);
5. проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;
6. оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);
7. определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

Правила и процедуры антивирусной защиты информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 21

к приказу

от15.08.2025 №01-11/331

Инструкция

по обновлению базы данных признаков вредоносных

компьютерных программ (вирусов)

Оператором должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

1. получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);
2. получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);
3. контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 22

к приказу

от15.08.2025 №01-11/331

Инструкция

по контролю установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

Оператором должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

Оператором должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

Контроль установки обновлений проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации и фиксируется в соответствующих журналах.

При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с АВЗ.2 (Приказа 21), баз решающих правил систем обнаружения вторжений в соответствии с СОВ.2 (Приказа 21), баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

Правила и процедуры контроля установки обновлений программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 23

к приказу

от15.08.2025 №01-11/331

Инструкция

по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации

В информационной системе должны обеспечиваться идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации, в соответствии с ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6 и ИАФ.7 (Приказа 21).

Виртуальная инфраструктура включает среду виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

В качестве компонентов виртуальной инфраструктуры необходимо, как минимум, рассматривать серверное оборудование, аппаратное обеспечение консолей управления, оборудование хранения данных, сетевое оборудование, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальное аппаратное обеспечение, виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенным для выполнения определенных функций в виртуальной инфраструктуре), программное обеспечение управления виртуальной инфраструктурой (в том числе гипервизором, настройками виртуальных машин, миграцией виртуальных машин, балансировкой нагрузки), служебные данные компонентов виртуальной инфраструктуры (настройки и иные служебные данные), средства резервного копирования компонентов среды виртуализации и средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

В качестве объектов доступа в виртуальной инфраструктуре необходимо, как минимум, рассматривать программное обеспечение управления виртуальной инфраструктурой, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальные контейнеры (зоны), виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенная для выполнения определенных функций в виртуальной инфраструктуре), средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре должны обеспечиваться:

1. идентификация и аутентификация администраторов управления средствами виртуализации;
2. идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;
3. блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;
4. защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерного доступа к ней, уничтожения или модифицирования;
5. защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;
6. идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с ИАФ.1 – ИАФ.7 (Приказа 21).

Приложение 24

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин

В информационной системе должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин, в соответствии с УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.12, УПД.13. (Приказа 21).

При реализации мер по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре должны обеспечиваться:

1. контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;
2. контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;
3. управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;
4. контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил).
5. Кроме того, меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать:
6. разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг);
7. разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам информационной системы, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа принятыми в информационной системе в целом.

Приложение 25

к приказу

от15.08.2025 №01-11/331

Инструкция

по контролю и управлению физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены

Оператором должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

Контроль и управление физическим доступом должны предусматривать:

1. определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
2. санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
3. учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Правила и процедуры контроля и управления физическим доступом регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 26

к приказу

от15.08.2025 №01-11/331

Инструкция

по размещению устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

Оператором должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства.

Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

Приложение 27

к приказу

от15.08.2025 №01-11/331

Инструкция

по обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

Оператором должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

Приложение 28

к приказу

от15.08.2025 №01-11/331

Инструкция

по блокированию сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя

или по его запросу

В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя.

Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы).

Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации в соответствии с ИАФ.1 (Приказа 21).

Правила и процедуры блокирования сеансов доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 29

к приказу

от15.08.2025 №01-11/331

Инструкция

по разрешению (запрету) действий пользователей, разрешенных до идентификации и аутентификации

Оператором должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к общедоступной информации (вебсайтам, порталам, иным общедоступным ресурсам). Также администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 30

к приказу

от15.08.2025 №01-11/331

Инструкция

по уничтожению (стиранию) или обезличиванию персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контролю уничтожения (стирания) или обезличивания

Оператором должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации должны быть разработаны оператором и включены в организационно-распорядительные документы по защите информации.

Приложение 31

к приказу

от15.08.2025 №01-11/331

Инструкция

по выявлению, анализу уязвимостей информационной системы и оперативному устранению вновь выявленных уязвимостей

Оператором должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе.

При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

1. выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
2. разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
3. анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
4. устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;
5. информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной оператором. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

Оператором должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей.

Правила и процедуры выявления, анализа и устранения уязвимостей регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 32

к приказу

от15.08.2025 №01-11/331

Инструкция

по контролю работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

Оператором должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

1. контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;
2. проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;
3. контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;
4. восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Приложение 33

к приказу

от15.08.2025 №01-11/331

Инструкция

по контролю состава технических средств, программного обеспечения и средств защиты информации

Оператором должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

1. контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;
2. контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
3. контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
4. исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Приложение 34

к приказу

от15.08.2025 №01-11/331

Инструкция

по регистрации событий безопасности в виртуальной инфраструктуре

В информационной системе должна обеспечиваться регистрация событий безопасности в виртуальной инфраструктуре в соответствии с РСБ.1, РСБ.2, РСБ.3, РСБ.4 и РСБ.5 (Приказа 21).

При реализации мер по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в РСБ.1 (Приказа 21), должны подлежать регистрации следующие события:

1. запуск (завершение) работы компонентов виртуальной инфраструктуры;
2. доступ субъектов доступа к компонентам виртуальной инфраструктуры;
3. изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;
4. изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры.

При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры.

При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период её аппаратного отключения состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры.

При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры.

Приложение 35

к приказу

от15.08.2025 №01-11/331

Инструкция

по реализации и управлению антивирусной защитой в виртуальной инфраструктуре

В информационной системе должны обеспечиваться реализация и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с АВЗ.1, АВЗ.2 (Приказа 21).

При реализации соответствующих мер должны обеспечиваться:

1. проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;
2. проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

Приложение 36

к приказу

от15.08.2025 №01-11/331

Инструкция

по разбиению виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей

В информационной системе должно обеспечиваться разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с ЗИС.17 (Приказа 21).

Приложение 37

к приказу

от15.08.2025 №01-11/331

Инструкция

по защите беспроводных соединений, применяемых в информационной системе

Оператором должна быть обеспечена защита беспроводных соединений, применяемых в информационной системе. Защита беспроводных соединений включает:

1. ограничение на использование в информационной системе беспроводных соединений (в частности 802.11хWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и иных беспроводных соединений) в соответствии с задачами (функциями) информационной системы, для решения которых такие соединения необходимы;
2. предоставление доступа к параметрам (изменению параметров) настройки беспроводных соединений только администраторам информационной системы;
3. обеспечение возможности реализации беспроводных соединений только через контролируемые интерфейсы (в том числе, путем применения средств защиты информации);
4. регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к информационной системе через беспроводные соединения.

При обеспечении защиты беспроводных соединений в зависимости от их типов должны реализовываться меры по идентификации и аутентификации в соответствии с ИАФ.1, ИАФ.2 и ИАФ.6 (Приказа 21).

При невозможности исключения установления беспроводных соединений из-за пределов контролируемой зоны должны приниматься меры защищенного удаленного доступа в соответствии с УПД.13 и ЗИС.3 (Приказа 21).

Правила и процедуры применения беспроводных соединений регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 38

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению конфигурацией информационной системы и системы защиты персональных данных

Оператором должно осуществляться управление конфигурацией информационной системы и системы защиты персональных данных. Управление конфигурацией информационной системы и системы защиты персональных данных включает:

1. определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;
2. управление изменениями конфигурации информационной системы и системы защиты персональных данных;
3. анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных;
4. документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных.

Приложение 39

к приказу

от15.08.2025 №01-11/331

Инструкция

по идентификации и аутентификации устройств, в том числе стационарных, мобильных и портативных

В информационной системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

Оператором должен быть определен перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, МАС-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

Аутентификация устройств в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

Правила и процедуры идентификации и аутентификации устройств регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 40

к приказу

от15.08.2025 №01-11/331

Инструкция

по обеспечению доверенной загрузки средств вычислительной техники

В информационной системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки.

Доверенная загрузка должна обеспечивать:

1. блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;
2. контроль доступа пользователей к процессу загрузки операционной системы;
3. контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

В информационной системе применяется доверенная загрузка на разных уровнях (уровня базовой системы ввода-вывода, уровня платы расширения и уровня загрузочной записи).

Правила и процедуры обеспечения доверенной загрузки средств вычислительной техники регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 41

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению установкой (инсталляцией) компонентов программного обеспечения, в том числе определению компонентов, подлежащих установке, настройке параметров установки компонентов, контролю за установкой компонентов программного обеспечения

Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы:

1. определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы;
2. настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения);
3. выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или не включение в домен);
4. контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов);
5. определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.

Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения (в том числе управления составом и конфигурацией подлежащих установке компонентов программного обеспечения, параметрами установки, параметрами настройки компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации с учетом эксплуатационной документации.

Приложение 42

к приказу

от15.08.2025 №01-11/331

Инструкция

по учету машинных носителей персональных данных

Оператором должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

Учету подлежат:

1. съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
2. портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
3. машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации.

Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски).

Приложение 43

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению доступом к машинным носителям персональных данных

Оператором должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в информационной системе:

1. определение должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим:
	1. съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
	2. портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
	3. машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);
2. предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

Правила и процедуры доступа к машинным носителям информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 44

к приказу

от15.08.2025 №01-11/331

Инструкция

по мониторингу (просмотр, анализ) результатов регистрации событий безопасности и реагированию на них

Оператором должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с РСБ.1 (Приказа 21), и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе.

В случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

Правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них регламентируются в организационно-распорядительных документах оператора по защите информации

Приложение 45

к приказу

от15.08.2025 №01-11/331

Инструкция

по обнаружению вторжений

Оператором должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений.

Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе информационной системы (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором.

Права по управлению (администрированию) системами обнаружения вторжений должны предоставляться только уполномоченным должностным лицам.

Системы обнаружения вторжений должны обеспечивать реагирование на обнаруженные и распознанные компьютерные атаки с учетом особенностей функционирования информационных систем.

Правила и процедуры обнаружения (предотвращения) вторжений (компьютерных атак) регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 46

к приказу

от15.08.2025 №01-11/331

Инструкция

по обновлению базы решающих правил

Оператором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе.

Обновление базы решающих правил системы обнаружения вторжений должно предусматривать:

1. получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;
2. получение из доверенных источников и установку обновлений базы решающих правил;
3. контроль целостности обновлений базы решающих правил.

Правила и процедуры обновления базы решающих правил регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 47

к приказу

от15.08.2025 №01-11/331

Инструкция

по контролю правил генерации и смены паролей пользователей, заведению и удалению учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе

Оператором должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

1. контроль правил генерации и смены паролей пользователей в соответствии с ИАФ.1 и ИАФ.4 (Приказа 21);
2. контроль заведения и удаления учетных записей пользователей в соответствии с УПД.1 (Приказа 21);
3. контроль реализации правил разграничения доступом в соответствии с УПД.2 (Приказа 21);
4. контроль реализации полномочий пользователей в соответствии с УПД.4 и УПД.5 (Приказа 21);
5. контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации оператора;
6. устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Приложение 48

к приказу

от15.08.2025 №01-11/331

Инструкция

по контролю целостности программного обеспечения, включая программное обеспечение средств защиты информации

В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать:

1. контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы; контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;
2. контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;
3. тестирование с периодичностью установленной оператором функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с АНЗ.1 и АНЗ.2 (Приказа 21);
4. обеспечение физической защиты технических средств информационной системы в соответствии с ЗТС.2 и ЗТС.3 (Приказа 21).

В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.

Правила и процедуры контроля целостности программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 49

к приказу

от15.08.2025 №01-11/331

Инструкция

по обнаружению и реагированию на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)

Оператором должно обеспечиваться обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

Защита от спама реализуется на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах и (или) мобильных технических средствах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам.

Защита от спама обеспечивается применением специализированных средств защиты, реализующих следующие механизмы защиты:

1. фильтрация по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами;
2. фильтрация на основе информации об отправителе электронного сообщения (в том числе с использованием «черных» списков (запрещенные отправители) и (или) «белых» списков (разрешенные отправители).

Оператором должно осуществляться обновление базы «черных» («белых») списков и контроль целостности базы «черных» («белых») списков.

Правила и процедуры обнаружения и реагирования на поступление незапрашиваемой информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 50

к приказу

от15.08.2025 №01-11/331

Инструкция

по периодическому резервному копированию персональных данных на резервные машинные носители персональных данных

Оператором должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:

1. резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью;
2. разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;
3. регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;
4. принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность.

Правила и процедуры резервного копирования информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 51

к приказу

от15.08.2025 №01-11/331

Инструкция

по обеспечению возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала

Оператором должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать:

1. определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации;
2. восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала;
3. регистрация событий, связанных восстановлением информации с резервных машинных носителей информации.

Правила и процедуры восстановления информации с резервных машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Приложение 52

к приказу

от15.08.2025 №01-11/331

Инструкция

по управлению перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных

Оператором должно обеспечиваться управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

При управлении перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных должны обеспечиваться:

1. регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);
2. управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);
3. управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации;
4. управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).
5. Управление перемещением виртуальных машин (контейнеров) должно предусматривать:
6. полный запрет перемещения виртуальных машин (контейнеров);
7. ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);
8. ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

Приложение 53

к приказу

от15.08.2025 №01-11/331

Инструкция

по контролю целостности виртуальной инфраструктуры и ее конфигураций

В информационной системе должен обеспечиваться контроль целостности компонентов виртуальной инфраструктуры в соответствии с ОЦЛ.1.

При реализации мер по контролю целостности компонентов виртуальной инфраструктуры должны обеспечиваться:

1. контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);
2. контроль целостности состава и конфигурации виртуального оборудования; контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;
3. контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться в то время, когда файлы-образы не задействованы).

В информационной системе должен обеспечиваться контроль целостности резервных копий виртуальных машин (контейнеров).

Приложение 54

к приказу

от15.08.2025 №01-11/331

Инструкция

по резервному копированию данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры

В информационной системе должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в соответствии с ОДТ.2, ОДТ.4, ОДТ.5 (Приказа 21).

При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры должны обеспечиваться:

1. определение мест хранения резервных копий виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре;
2. резервное копирование виртуальных машин (контейнеров);
3. резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;
4. резервирование программного обеспечения виртуальной инфраструктуры;
5. резервирование каналов связи, используемых в виртуальной инфраструктуре;
6. периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.

Приложение 55

к приказу

от15.08.2025 №01-11/331

Инструкция

по обеспечению подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов

В информационной системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»).

Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены должна осуществляться их аутентификация в соответствии с ИАФ.2 и ЗИС.10 (Приказа 21).

Контроль целостности передаваемой информации должен включать проверку целостности передаваемых пакетов (в частности в соответствии с ЗИС.3) (Приказа 21).

Приложение 56

к приказу

от15.08.2025 №01-11/331

Инструкция

по защите архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных

В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, определенных оператором в соответствии с настоящим методическим документом, направленных на обеспечение их конфиденциальности и целостности.

Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.

Приложение 57

к приказу

от15.08.2025 №01-11/331

Инструкция

по разбиению информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы

Оператором должно осуществляться разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечиваться защита периметров сегментов информационной системы.

Сегментирование информационной системы проводится с целью построения многоуровневой (эшелонированной) системы защиты информации путем построения сегментов на различных физических доменах или средах. Принципы сегментирования информационной системы определяются оператором с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации и должны заключаться в снижении вероятности реализации угроз и (или) их локализации в рамках одного сегмента.

Сегментирование информационной системы также может проводиться с целью разделения информационной системы на сегменты, имеющие различные классы защищенности информационной системы.

При сегментировании информационной системы должна быть обеспечена защита периметров сегментов информационной системы в соответствии с УПД.3 и ЗИС.23 (Приказа 21).

Приложение 58

к приказу

от15.08.2025 №01-11/331

Инструкция

по выявлению инцидентов и реагированию на них

Оператором должны выполняться мероприятия по выявлению инцидентов и реагированию на них. Выявление инцидентов и реагирование на них включает:

1. определение лиц, ответственных за выявление инцидентов и реагирование на них;
2. обнаружение, идентификация и регистрация инцидентов;
3. своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;
4. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
5. принятие мер по устранению последствий инцидентов;
6. планирование и принятие мер по предотвращению повторного возникновения инцидентов.