Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (Зарегистрировано в Минюсте России 14.05.2013 N 28375)

Зарегистрировано в Минюсте России 14 мая 2013 г. N 28375

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 18 февраля 2013 г. N 21

ОБ УТВЕРЖДЕНИИ СОСТАВА И СОДЕРЖАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; 2011, N 23, ст. 3263; N 31, ст. 4701) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818), приказываю:

1. Утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Признать утратившим силу приказ ФСТЭК России от 5 февраля 2010 г. N 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных" (зарегистрирован Минюстом России 19 февраля 2010 г., регистрационный N 16456).

Директор
Федеральной службы по техническому
и экспортному контролю
В.СЕЛИН

Утверждены
приказом ФСТЭК России
от 18 февраля 2013 г. N 21

СОСТАВ И СОДЕРЖАНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

I. Общие положения

1. Настоящий документ разработан в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; 2011, N 23, ст. 3263; N 31, ст. 4701) и устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - меры по обеспечению безопасности персональных данных) для каждого из уровней защищенности персональных данных, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования,

копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

В настоящем документе не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также меры, связанные с применением шифровальных (криптографических) средств защиты информации.

2. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

3. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

КонсультантПлюс: примечание.
Нумерация пунктов дана в соответствии с официальным текстом документа.

6. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года.

7. Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2010, N 31, ст. 4196; 2011, N 15, ст. 2038; N 30, ст. 4600; 2012, N 31, ст. 4328).

II. Состав и содержание мер по обеспечению безопасности персональных данных

8. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;
защита среды виртуализации;
защита технических средств;
защита информационной системы, ее средств, систем связи и передачи данных;
выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к настоящему документу.

8.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

8.2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

8.3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

8.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

8.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

8.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.7. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

8.8. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

8.9. Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

8.10. Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

8.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему

хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

8.12. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

8.13. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

8.14. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

8.15. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

9. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в приложении к настоящему документу;

адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

10. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

11. В случае определения в соответствии с Требованиями к защите персональных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119, в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

тестирование информационной системы на проникновения;

использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

12. При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

а) для обеспечения 1 и 2 уровней защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

б) для обеспечения 3 уровня защищенности персональных данных применяются:

средства вычислительной техники не ниже 5 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса защиты в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и межсетевые экраны не ниже 4 класса в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

в) для обеспечения 4 уровня защищенности персональных данных применяются:

средства вычислительной техники не ниже 6 класса;

системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

межсетевые экраны 5 класса.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

13. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

Приложение
к Составу и содержанию
организационных и технических
мер по обеспечению безопасности
персональных данных при их
обработке в информационных
системах персональных данных

СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, НЕОБХОДИМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ КАЖДОГО ИЗ УРОВНЕЙ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Условное обозначение и номер меры Содержание мер по обеспечению безопасности персональных данных

Уровни защищенности персональных данных			
4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1			
Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+
ИАФ.2			
Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	+	+	
ИАФ.3			
Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+
ИАФ.4			
Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+
ИАФ.5			
Защита обратной связи при вводе аутентификационной информации	+	+	+
ИАФ.6			
Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1			
Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+
УПД.2			
Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+

+
УПД.3
Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
+
+
+
+
УПД.4
Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
+
+
+
+
УПД.5
Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
+
+
+
+
УПД.6
Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
+
+
+
+
УПД.7
Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных
УПД.8
Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему
УПД.9
Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы
УПД.10
Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
+
+
+
УПД.11
Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
+
+
+
УПД.12
Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки
УПД.13
Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

				+
				+
				+
				+
УПД.14				
Регламентация и контроль использования в информационной системе технологий беспроводного доступа				
				+
				+
				+
				+
УПД.15				
Регламентация и контроль использования в информационной системе мобильных технических средств				
				+
				+
				+
				+
УПД.16				
Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)				
				+
				+
				+
				+
УПД.17				
Обеспечение доверенной загрузки средств вычислительной техники				
				+
				+
III. Ограничение программной среды (ОПС)				
ОПС.1				
Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2				
Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения				
				+
				+
ОПС.3				
Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				
				+
ОПС.4				
Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей персональных данных (ЗНИ)				
ЗНИ.1				
Учет машинных носителей персональных данных				
				+
				+
ЗНИ.2				
Управление доступом к машинным носителям персональных данных				
				+
				+
ЗНИ.3				

Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны	ЗНИ.4			
Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах	ЗНИ.5			
Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных	ЗНИ.6			
Контроль ввода (вывода) информации на машинные носители персональных данных	ЗНИ.7			
Контроль подключения машинных носителей персональных данных	ЗНИ.8			
Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	+	+	+	
V. Регистрация событий безопасности (РСБ)				
Определение событий безопасности, подлежащих регистрации, и сроков их хранения	РСБ.1	+	+	+
Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	РСБ.2	+	+	+
Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	РСБ.3	+	+	+
Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	РСБ.4			
Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	РСБ.5	+	+	
Генерирование временных меток и (или) синхронизация системного времени в информационной системе	РСБ.6			
Защита информации о событиях безопасности	РСБ.7	+	+	+

			+	
		VI. Антивирусная защита (АВЗ)		
		АВЗ.1		
Реализация антивирусной защиты			+	
			+	
			+	
			+	
		АВЗ.2		
Обновление базы данных признаков вредоносных компьютерных программ (вирусов)			+	
			+	
			+	
			+	
		VII. Обнаружение вторжений (СОВ)		
		СОВ.1		
Обнаружение вторжений			+	
			+	
		СОВ.2		
Обновление базы решающих правил			+	
			+	
		VIII. Контроль (анализ) защищенности персональных данных (АНЗ)		
		АНЗ.1		
Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей			+	
			+	
			+	
		АНЗ.2		
Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации			+	
			+	
			+	
			+	
		АНЗ.3		
Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации			+	
			+	
			+	
		АНЗ.4		
Контроль состава технических средств, программного обеспечения и средств защиты информации			+	
			+	
			+	
		АНЗ.5		
Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	
			+	
		IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)		
		ОЦЛ.1		
Контроль целостности программного обеспечения, включая программное обеспечение средств				

защиты информации				
	+			
	+			
ОЦЛ.2				
Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3				
Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4				
Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)				
	+			
	+			
ОЦЛ.5				
Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6				
Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7				
Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8				
Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)				
ОДТ.1				
Использование отказоустойчивых технических средств				
ОДТ.2				
Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3				
Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				
	+			
ОДТ.4				
Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных				
	+			
	+			
ОДТ.5				
Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала				
	+			
	+			
XI. Защита среды виртуализации (ЗСВ)				
ЗСВ.1				
Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации				
	+			
	+			
	+			
	+			
ЗСВ.2				
Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том				

числе внутри виртуальных машин	+	+	+
ЗСВ.3			
Регистрация событий безопасности в виртуальной инфраструктуре	+	+	+
ЗСВ.4			
Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры			
ЗСВ.5			
Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией			
ЗСВ.6			
Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+	+	
ЗСВ.7			
Контроль целостности виртуальной инфраструктуры и ее конфигураций	+	+	
ЗСВ.8			
Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	+	+	
ЗСВ.9			
Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	+	+
ЗСВ.10			
Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	+	+	+
XII. Защита технических средств (ЗТС)			
ЗТС.1			
Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам			
ЗТС.2			
Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования			
ЗТС.3			
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, в помещения и сооружения, в которых они установлены	+		

				+
				+
				+
ЗТС.4				
Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр				
				+
				+
				+
				+
ЗТС.5				
Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
ЗИС.1				
Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				
				+
ЗИС.2				
Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3				
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				
				+
				+
				+
				+
ЗИС.4				
Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС.5				
Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6				
Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС.7				
Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС.8				
Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9				
Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10				
Подтверждение происхождения источника информации, получаемой в процессе определения сетевых				

адресов по сетевым именам или определения сетевых имен по сетевым адресам			
ЗИС.11			
Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	+	+	
ЗИС.12			
Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю			
ЗИС.13			
Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя			
ЗИС.14			
Использование устройств терминального доступа для обработки персональных данных			
ЗИС.15			
Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных	+	+	
ЗИС.16			
Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов			
ЗИС.17			
Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	+	+	
ЗИС.18			
Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения			
ЗИС.19			
Изоляция процессов (выполнение программ) в выделенной области памяти			
ЗИС.20			
Защита беспроводных соединений, применяемых в информационной системе	+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)			
ИНЦ.1			
Определение лиц, ответственных за выявление инцидентов и реагирование на них	+	+	
ИНЦ.2			
Обнаружение, идентификация и регистрация инцидентов	+	+	
ИНЦ.3			
Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	+	+	
ИНЦ.4			
Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	+	+	
ИНЦ.5			

Принятие мер по устранению последствий инцидентов + + ИНЦ.6 Планирование и принятие мер по предотвращению повторного возникновения инцидентов + +					
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.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		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

"+" - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.