Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы		
		3	2	1
1. Идентификация и аутентификация (ИАФ)				
ИАФ.1	Идентификация пользователей	+	+ 1	+ 1
ИАФ.2	Идентификация устройств			
ИАФ.3	Аутентификация пользователей	+	+	+ 1
ИАФ.4	Аутентификация устройств			
2. Управление доступом (УПД)				
УПД.1	Реализация модели управления доступом	+ 1	+ 1, 2	+ 1, 2
УПД.2	Разграничение и контроль прав доступа	+	+ 1, 2	+ 1, 2
УПД.3	Управление учетными записями	+	+ 1	+ 1, 2
УПД.4	Ограничение неуспешных и нерегламентированных попыток доступа в информационную систему	+	+ 1, 2	+ 1, 2
УПД.5	Предупреждение пользователя при его доступе к информационной системе			
УПД.6	Оповещение пользователя о предыдущем входе в информационную систему			
УПД.7	Ограничение числа параллельных сеансов доступа		+	+ 1а
УПД.8	Блокирование сеанса доступа пользователя при неактивности	+	+	+
УПД.9	Контроль действий субъектов доступа до идентификации и аутентификации	+	+	+
3. Регистрация событий безопасности (РСБ)				
РСБ.1	Определение событий безопасности и данных о них, подлежащих регистрации	+ 1	+ 1,2	+ 1, 2, 3
РСБ.2	Анализ событий безопасности и реагирование на них	+	+	+
РСБ.3	Генерация временных меток при регистрации событий безопасности	+	+	+
РСБ.4	Требования к сбору, хранению и защите данных о событиях безопасности	+	+	+
РСБ.5	Реагирование на сбои при регистрации событий безопасности	+	+	+
4. Защита виртуализации облачных технологий (ЗСВ)				
ЗСВ.1	Доверенная загрузка средства виртуализации и виртуальных машин	+	+ 1	+ 1, 2
ЗСВ.2	Контроль целостности средства виртуализации и виртуальных машин	+	+ 1, 2	+ 1, 2

ЗСВ.3	Регистрация событий безопасности в среде вирутализации	+	+	+
ЗСВ.4	Управление доступом в среде виртуализации	+	+	+
ЗСВ.5	Резервное копирование в среде виртуализации	+	+	+
ЗСВ.6	Ограничение программной среды в среде виртуализации	+	+	+ 1
ЗСВ.7	Защита памяти в среде виртуализации	+	+	+
ЗСВ.8	Идентификация и аутентификация в среде виртуализации	+	+	+
ЗСВ.9	Управление виртуальными машинами		+	+
5. Защита контейнерных сред и их оркестрации (ЗКО)				
ЗКО.1	Контроль целостности в контейнерных средах	+	+ 1, 2	+ 1, 2, 3, 4, 5, 6
ЗКО.2	Регистрация событий безопасности в контейнерных средах	+	+	+
ЗКО.3	Управление доступом в контейнерных средах	+	+	+
ЗКО.4	Резервное копирование в контейнерных средах	+	+	+
ЗКО.5	Изоляция контейнеров в контейнерной среде	+	+ 1	+ 1
ЗКО.6	Идентификация и аутентификация в контейнерной среде	+	+	+
ЗКО.7	Управление контейнерами и их образами (оркестрация)	+	+	+
ЗКО.8	Выявление уязвимостей в контейнерной среде	+	+ 1,2	+ 1,2
6. Защита сервисов электронной почты (ЗЭП)				
ЗЭП.1	Защита ящиков и сообщений электронной почты	+	+	+
ЗЭП.2	Контроль доступа пользователей	+	+	+
ЗЭП.3	Защита от вредоносных вложений	+	+ 1	+ 1
ЗЭП.4	Защита от фишинга	+	+ 1	+ 1
ЗЭП.5	Защита от спама	+	+	+
ЗЭП.6	Защита метаданных и иной технической информации сервисов электронной почты	+	+	+
7. Защита веб-технологий (ЗВТ)				
ЗВТ.1	Защита пользовательских данных	+	+	+
ЗВТ.2	Контроль доступа пользователей	+	+ 1	+ 1
ЗВТ.3	Контроль и фильтрация трафика веб-приложений	+	+	+ 1
ЗВТ.4	Регистрация событий безопасности в веб-приложениях и реагирование на них	+	+	+
ЗВТ.5	Проверка файлов веб-приложений на вредоносное программное обеспечение	+	+	+

8. Защита программных интерфейсов взаимодействия приложений API (ЗПИ)				
ЗПИ.1	Защита данных API	+	+ 1	+ 1
ЗПИ.2	Управление доступом пользователей и приложений	+	+	+
ЗПИ.3	Проверка на соответствие спецификации API	+	+	+ 1
9. Защита конечных устройств (ЗКУ)				
ЗКУ.1	Управление доступом к конечным устройствам	+	+	+
ЗКУ.2	Обеспечение целостности программного обеспечения конечного устройства	+	+ 1,2	+ 1,2
ЗКУ.3	Антивирусная защита и обнаружение и предотвращение вторжений на конечных устройствах	+	+ 1	+ 1
ЗКУ.4	Мониторинг процессов и состояния устройства	+	+ 1	+ 1
ЗКУ.5	Контроль и фильтрация трафика на устройстве	+	+	+
ЗКУ.6	Анализ и реагирование на события безопасности	+	+ 1	+ 1
10. Защита мобильных устройств (ЗМУ)				
ЗМУ.1	Идентификация и аутентификация пользователей	+	+ 1	+ 1
ЗМУ.2	Контроль доступа	+	+	+
ЗМУ.3	Контроль целостности	+	+ 1	+ 1, 2
ЗМУ.4	Защита данных	+	+	+ 1, 2
ЗМУ.5	Антивирусная защита	+	+	+
ЗМУ.6	Контроль приложений	+	+	+
ЗМУ.7	Ограничение и контроль функциональности	+	+	+
ЗМУ.8	Определение и контроль геопозиции	+	+ 1	+ 1
ЗМУ.9	Регистрация, анализ и реагирование на события безопасности	+	+ 1	+ 1
11. Защита устройств «Интернета вещей» (ЗИВ)				
ЗИВ.1	Идентификация и аутентификация	+	+	+
ЗИВ.2	Управление доступом	+	+	+
ЗИВ.3	Защита данных	+	+ 1	+ 1
ЗИВ.4	Контроль целостности	+	+	+
ЗИВ.5	Регистрация, анализ и реагирование на события безопасности	+	+ 1	+ 1
12. Защита точек беспроводного доступа (ЗБД)				
ЗБД.1	Идентификация и аутентификация	+	+	+ 1
ЗБД.2	Контроль доступа	+	+	+
ЗБД.3	Защита пользовательских данных	+	+	+
ЗБД.4	Контроль целостности	+	+	+
ЗБД.5	Ограничение уровней сигналов	+	+	+

ЗБД.6	Регистрация, анализ и реагирование на события безопасности	+	+ 1	+ 1
13. Антивирусная защита (АВЗ)				
АВЗ.1	Антивирусная защита устройств и серверов	+	+	+
АВЗ.2	Антивирусная защита электронной почты	+	+	+
АВЗ.3	Антивирусная проверка сетевого трафика	+	+	+
АВЗ.4	Применение замкнутой программной среды исполнения («песочницы»)			
14. Обнаружение и предотвращение вторжений на сетевом уровне (СОВ)				
СОВ.1	Обнаружение и предотвращение вторжений на периметре	+	+ 1	+ 1
СОВ.2	Обнаружение и предотвращение вторжений в сегментах информационной системы	+	+	+
15. Сегментация и межсетевое экранирование (МСЭ)				
МСЭ.1	Сегментация сети	+	+	+ 1
МСЭ.2	Организация демилитаризованной зоны	+	+	+
МСЭ.3	Контроль сетевого доступа и фильтрация трафика	+	+	+
МСЭ.4	Маскирование системы			
МСЭ.5	Создание ложных систем			
16. Защита от атак, направленных на отказ в обслуживании (ЗОО)				
ЗОО.1	Защита от компьютерных атак, направленных на отказ в обслуживании, при доступе внешних пользователей к прикладным сервисам, предоставляемым информационной системой	+	+	+
ЗОО.2	Контроль и фильтрация входящего трафика	+	+	+ 1
ЗОО.3	Мониторинг состояния сервисов и интерфейсов	+	+	+
ЗОО.4	Балансировка нагрузки			
ЗОО.5	Ограничение нагрузки	+	+	+
ЗОО.6	Поддержка резерва достаточной пропускной способности и расширение ресурсов при сбоях	+	+	+
17. Защита каналов связи и сетевого взаимодействия (ЗКС)				
ЗКС.1	Защита данных при передаче по каналам связи	+	+	+
ЗКС.2	Контроль атрибутов безопасности при сетевом взаимодействии	+	+	+
ЗКС.3	Контроль доступа к внешним ресурсам	+	+	+
ЗКС.4	Контекстная проверка исходящего трафика			