Раздел	Приказ	Код	Меры защиты и обеспечения безопасности	4	3	2	1
0	**Приказ 17**		**Меры защиты информации в информационных системах**		**Классы защищенности ИС**		
0	**Приказ 21**		**Содержание мер по обеспечению безопасности персональных данных**	**Уровни защищенности ПДн**			
0	**Приказ 31**		**Меры защиты информации в автоматизированных системах управления**		**Классы защищенности АСУ**		
0	**Приказ 239**		**Меры обеспечения безопасности значимого объекта**		**Категория значимости**		
1	**Приказ 17**	**I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)**					
1	**Приказ 21**	**I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)**					
1	**Приказ 31**	**I. Идентификация и аутентификация (ИАФ)**					
1	**Приказ 239**	**I. Идентификация и аутентификация (ИАФ)**					
1	**Приказ 31**	ИАФ.0	Разработка политики идентификации и аутентификации		+	+	+
1	**Приказ 239**	ИАФ.0	Регламентация правил и процедур идентификации и аутентификации		+	+	+
1	**Приказ 17**	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора		+	+	+
1	**Приказ 21**	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
1	**Приказ 31**	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов		+	+	+
1	**Приказ 239**	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов		+	+	+
1	**Приказ 17**	ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
1	**Приказ 21**	ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
1	**Приказ 31**	ИАФ.2	Идентификация и аутентификация устройств		+	+	+
1	**Приказ 239**	ИАФ.2	Идентификация и аутентификация устройств		+	+	+
1	**Приказ 17**	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов		+	+	+
1	**Приказ 21**	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
1	**Приказ 31**	ИАФ.3	Управление идентификаторами		+	+	+
1	**Приказ 239**	ИАФ.3	Управление идентификаторами		+	+	+
1	**Приказ 17**	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		+	+	+
1	**Приказ 21**	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	+	+	+	+
1	**Приказ 31**	ИАФ.4	Управление средствами аутентификации		+	+	+
1	**Приказ 239**	ИАФ.4	Управление средствами аутентификации		+	+	+
1	**Приказ 17**	ИАФ.5	Защита обратной связи при вводе аутентификационной информации		+	+	+
1	**Приказ 21**	ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
1	**Приказ 31**	ИАФ.5	Идентификация и аутентификация внешних пользователей		+	+	+
1	**Приказ 239**	ИАФ.5	Идентификация и аутентификация внешних пользователей		+	+	+
1	**Приказ 17**	ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)		+	+	+
1	**Приказ 21**	ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
1	**Приказ 31**	ИАФ.6	Двусторонняя аутентификация				
1	**Приказ 239**	ИАФ.6	Двусторонняя аутентификация				
1	**Приказ 17**	ИАФ.7	Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа				
1	**Приказ 31**	ИАФ.7	Защита аутентификационной информации при передаче		+	+	+
1	**Приказ 239**	ИАФ.7	Защита аутентификационной информации при передаче		+	+	+
2	**Приказ 17**	**II. Управление доступом субъектов доступа к объектам доступа (УПД)**					
2	**Приказ 21**	**II. Управление доступом субъектов доступа к объектам доступа (УПД)**					
2	**Приказ 31**	**II. Управление доступом (УПД)**					
2	**Приказ 239**	**II. Управление доступом (УПД)**					

2	**Приказ 31**	УПД.0	Разработка политики управления доступом		+	+	+
2	**Приказ 239**	УПД.0	Регламентация правил и процедур управления доступом		+	+	+
2	**Приказ 17**	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей		+	+	+
2	**Приказ 21**	УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
2	**Приказ 31**	УПД.1	Управление учетными записями пользователей		+	+	+
2	**Приказ 239**	УПД.1	Управление учетными записями пользователей		+	+	+
2	**Приказ 17**	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа		+	+	+
2	**Приказ 21**	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
2	**Приказ 31**	УПД.2	Реализация политик управления доступа		+	+	+
2	**Приказ 239**	УПД.2	Реализация модели управления доступом		+	+	+
2	**Приказ 17**	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		+	+	+
2	**Приказ 21**	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	+	+	+	+
2	**Приказ 31**	УПД.3	Доверенная загрузка			+	+
2	**Приказ 239**	УПД.3	Доверенная загрузка			+	+
2	**Приказ 17**	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы		+	+	+
2	**Приказ 21**	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
2	**Приказ 31**	УПД.4	Разделение полномочий (ролей) пользователей		+	+	+
2	**Приказ 239**	УПД.4	Разделение полномочий (ролей) пользователей		+	+	+
2	**Приказ 17**	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы		+	+	+
2	**Приказ 21**	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
2	**Приказ 31**	УПД.5	Назначение минимально необходимых прав и привилегий		+	+	+
2	**Приказ 239**	УПД.5	Назначение минимально необходимых прав и привилегий		+	+	+
2	**Приказ 17**	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)		+	+	+
2	**Приказ 21**	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
2	**Приказ 31**	УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему		+	+	+
2	**Приказ 239**	УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему		+	+	+
2	**Приказ 17**	УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации				
2	**Приказ 21**	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				
2	**Приказ 31**	УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам				
2	**Приказ 239**	УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам				
2	**Приказ 17**	УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
2	**Приказ 21**	УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
2	**Приказ 31**	УПД.8	Оповещение пользователя при успешном входе предыдущем доступе к информационной (автоматизированной) системе				+
2	**Приказ 239**	УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе				

2	**Приказ 17**	УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				+
2	**Приказ 21**	УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
2	**Приказ 31**	УПД.9	Ограничение числа параллельных сеансов доступа				+
2	**Приказ 239**	УПД.9	Ограничение числа параллельных сеансов доступа				+
2	**Приказ 17**	УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
2	**Приказ 21**	УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
2	**Приказ 31**	УПД.10	Блокирование сеанса доступа пользователя при неактивности		+	+	+
2	**Приказ 239**	УПД.10	Блокирование сеанса доступа пользователя при неактивности		+	+	+
2	**Приказ 17**	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
2	**Приказ 21**	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
2	**Приказ 31**	УПД.11	Управление действиями пользователей до идентификации и аутентификации		+	+	+
2	**Приказ 239**	УПД.11	Управление действиями пользователей до идентификации и аутентификации		+	+	+
2	**Приказ 17**	УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
2	**Приказ 21**	УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
2	**Приказ 31**	УПД.12	Управление атрибутами безопасности				
2	**Приказ 239**	УПД.12	Управление атрибутами безопасности				
2	**Приказ 17**	УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети		+	+	+
2	**Приказ 21**	УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
2	**Приказ 31**	УПД.13	Реализация защищенного удаленного доступа		+	+	+
2	**Приказ 239**	УПД.13	Реализация защищенного удаленного доступа		+	+	+
2	**Приказ 17**	УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа		+	+	+
2	**Приказ 21**	УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
2	**Приказ 31**	УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем		+	+	+
2	**Приказ 239**	УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем		+	+	+
2	**Приказ 17**	УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств		+	+	+
2	**Приказ 21**	УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
2	**Приказ 17**	УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)		+	+	+
2	**Приказ 21**	УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
2	**Приказ 17**	УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
2	**Приказ 21**	УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
3	**Приказ 17**	**III. Ограничение программной среды (ОПС)**					
3	**Приказ 21**	**III. Ограничение программной среды (ОПС)**					
3	**Приказ 31**	**III. Ограничение программной среды (ОПС)**					
3	**Приказ 239**	**III. Ограничение программной среды (ОПС)**					
3	**Приказ 31**	ОПС.0	Разработка политики ограничения программной среды			+	+
3	**Приказ 239**	ОПС.0	Регламентация правил и процедур ограничения программной среды			+	+
3	**Приказ 17**	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				+
3	**Приказ 21**	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
3	**Приказ 31**	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения				+
3	**Приказ 239**	ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения				+

3	**Приказ 17**	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			+	+
3	**Приказ 21**	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			+	+
3	**Приказ 31**	ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения			+	+
3	**Приказ 239**	ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения			+	+
3	**Приказ 17**	ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов		+	+	+
3	**Приказ 21**	ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
3	**Приказ 31**	ОПС.3	Управление временными файлами				
3	**Приказ 239**	ОПС.3	Управление временными файлами				
3	**Приказ 17**	ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
3	**Приказ 21**	ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
4	**Приказ 17**	**IV. Защита машинных носителей информации (ЗНИ)**					
4	**Приказ 21**	**IV. Защита машинных носителей персональных данных (ЗНИ)**					
4	**Приказ 31**	**IV. Защита машинных носителей информации (ЗНИ)**					
4	**Приказ 239**	**IV. Защита машинных носителей информации (ЗНИ)**					
4	**Приказ 31**	ЗНИ.0	Разработка политики защиты машинных носителей информации		+	+	+
4	**Приказ 239**	ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации		+	+	+
4	**Приказ 17**	ЗНИ.1	Учет машинных носителей информации		+	+	+
4	**Приказ 21**	ЗНИ.1	Учет машинных носителей персональных данных			+	+
4	**Приказ 31**	ЗНИ.1	Учет машинных носителей информации		+	+	+
4	**Приказ 239**	ЗНИ.1	Учет машинных носителей информации		+	+	+
4	**Приказ 17**	ЗНИ.2	Управление доступом к машинным носителям информации		+	+	+
4	**Приказ 21**	ЗНИ.2	Управление доступом к машинным носителям персональных данных			+	+
4	**Приказ 31**	ЗНИ.2	Управление физическим доступом к машинным носителям информации		+	+	+
4	**Приказ 239**	ЗНИ.2	Управление физическим доступом к машинным носителям информации		+	+	+
4	**Приказ 17**	ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				
4	**Приказ 21**	ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
4	**Приказ 31**	ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				
4	**Приказ 239**	ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				
4	**Приказ 17**	ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах				
4	**Приказ 21**	ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных,хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных				
4	**Приказ 31**	ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации				
4	**Приказ 239**	ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации				
4	**Приказ 17**	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации			+	+
4	**Приказ 21**	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
4	**Приказ 31**	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации		+	+	+
4	**Приказ 239**	ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации		+	+	+
4	**Приказ 17**	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации				
4	**Приказ 21**	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных				
4	**Приказ 31**	ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации				+

4	Приказ 239	ЗНИ.6	Контроль ввода (вывода) информации на съемные машинные носители информации				+
4	Приказ 17	ЗНИ.7	Контроль подключения машинных носителей информации				
4	Приказ 21	ЗНИ.7	Контроль подключения машинных носителей персональных данных				
4	Приказ 31	ЗНИ.7	Контроль подключения машинных носителей информации		+	+	+
4	Приказ 239	ЗНИ.7	Контроль подключения съемных машинных носителей информации		+	+	+
4	Приказ 17	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)		+	+	+
4	Приказ 21	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		+	+	+
4	Приказ 31	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации		+	+	+
4	Приказ 239	ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации		+	+	+
5	Приказ 31	**V. Аудит безопасности (АУД)**					
5	Приказ 239	**V. Аудит безопасности (АУД)**					
5	Приказ 31	АУД.0	Разработка политики аудита безопасности		+	+	+
5	Приказ 239	АУД.0	Регламентация правил и процедур аудита безопасности		+	+	+
5	Приказ 31	АУД.1	Инвентаризация информационных ресурсов		+	+	+
5	Приказ 239	АУД.1	Инвентаризация информационных ресурсов		+	+	+
5	Приказ 31	АУД.2	Анализ уязвимостей и их устранение		+	+	+
5	Приказ 239	АУД.2	Анализ уязвимостей и их устранение		+	+	+
5	Приказ 31	АУД.3	Генерирование временных меток и (или) синхронизация системного времени		+	+	+
5	Приказ 239	АУД.3	Генерирование временных меток и (или) синхронизация системного времени		+	+	+
5	Приказ 31	АУД.4	Регистрация событий безопасности		+	+	+
5	Приказ 239	АУД.4	Регистрация событий безопасности		+	+	+
5	Приказ 31	АУД.5	Контроль и анализ сетевого трафика				+
5	Приказ 239	АУД.5	Контроль и анализ сетевого трафика				+
5	Приказ 31	АУД.6	Защита информации о событиях безопасности		+	+	+
5	Приказ 239	АУД.6	Защита информации о событиях безопасности		+	+	+
5	Приказ 31	АУД.7	Мониторинг безопасности		+	+	+
5	Приказ 239	АУД.7	Мониторинг безопасности		+	+	+
5	Приказ 31	АУД.8	Реагирование на сбои при регистрации событий безопасности		+	+	+
5	Приказ 239	АУД.8	Реагирование на сбои при регистрации событий безопасности		+	+	+
5	Приказ 31	АУД.9	Анализ действий пользователей				+
5	Приказ 239	АУД.9	Анализ действий отдельных пользователей				+
5	Приказ 31	АУД.10	Проведение внутренних аудитов		+	+	+
5	Приказ 239	АУД.10	Проведение внутренних аудитов		+	+	+
5	Приказ 31	АУД.11	Проведение внешних аудитов				+
5	Приказ 239	АУД.11	Проведение внешних аудитов				
5	Приказ 17	**V. Регистрация событий безопасности (РСБ)**					
5	Приказ 21	**V. Регистрация событий безопасности (РСБ)**					
5	Приказ 17	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения		+	+	+
5	Приказ 21	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
5	Приказ 17	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации		+	+	+
5	Приказ 21	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
5	Приказ 17	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения		+	+	+
5	Приказ 21	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
5	Приказ 17	РСБ.4	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		+	+	+
5	Приказ 21	РСБ.4	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				
5	Приказ 17	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них		+	+	+

5	**Приказ 21**	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
5	**Приказ 17**	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе		+	+	+
5	**Приказ 21**	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
5	**Приказ 17**	РСБ.7	Защита информации о событиях безопасности		+	+	+
5	**Приказ 21**	РСБ.7	Защита информации о событиях безопасности	+	+	+	+
5	**Приказ 17**	РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе				
6	**Приказ 17**	**VI. Антивирусная защита (АВЗ)**					
6	**Приказ 21**	**VI. Антивирусная защита (АВЗ)**					
6	**Приказ 31**	**VI. Антивирусная защита (АВЗ)**					
6	**Приказ 239**	**VI. Антивирусная защита (АВЗ)**					
6	**Приказ 31**	АВЗ.0	Разработка политики антивирусной защиты		+	+	+
6	**Приказ 239**	АВЗ.0	Регламентация правил и процедур антивирусной защиты		+	+	+
6	**Приказ 17**	АВЗ.1	Реализация антивирусной защиты		+	+	+
6	**Приказ 21**	АВЗ.1	Реализация антивирусной защиты	+	+	+	+
6	**Приказ 31**	АВЗ.1	Реализация антивирусной защиты		+	+	+
6	**Приказ 239**	АВЗ.1	Реализация антивирусной защиты		+	+	+
6	**Приказ 17**	АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)		+	+	+
6	**Приказ 21**	АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
6	**Приказ 31**	АВЗ.2	Антивирусная защита электронной почты и иных сервисов		+	+	+
6	**Приказ 239**	АВЗ.2	Антивирусная защита электронной почты и иных сервисов		+	+	+
6	**Приказ 31**	АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов				+
6	**Приказ 239**	АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов				+
6	**Приказ 31**	АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)		+	+	+
6	**Приказ 239**	АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)		+	+	+
6	**Приказ 31**	АВЗ.5	Использование средств антивирусной защиты различных производителей				+
6	**Приказ 239**	АВЗ.5	Использование средств антивирусной защиты различных производителей				+
7	**Приказ 17**	**VII. Обнаружение вторжений (СОВ)**					
7	**Приказ 21**	**VII. Обнаружение вторжений (СОВ)**					
7	**Приказ 31**	**VII. Предотвращение вторжений (компьютерных атак) (СОВ)**					
7	**Приказ 239**	**VII. Предотвращение вторжений (компьютерных атак) (СОВ)**					
7	**Приказ 31**	СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)			+	+
7	**Приказ 239**	СОВ.0	Регламентация правил и процедур предотвращения вторжений (компьютерных атак)			+	+
7	**Приказ 17**	СОВ.1	Обнаружение вторжений			+	+
7	**Приказ 21**	СОВ.1	Обнаружение вторжений			+	+
7	**Приказ 31**	СОВ.1	Обнаружение и предотвращение компьютерных атак			+	+
7	**Приказ 239**	СОВ.1	Обнаружение и предотвращение компьютерных атак			+	+
7	**Приказ 17**	СОВ.2	Обновление базы решающих правил			+	+
7	**Приказ 31**	СОВ.2	Обновление базы решающих правил			+	+
7	**Приказ 239**	СОВ.2	Обновление базы решающих правил			+	+
7	**Приказ 21**	СОВ.2	Обновление базы решающих правил			+	+
8	**Приказ 17**	**VIII. Контроль (анализ) защищенности информации (АНЗ)**					
8	**Приказ 21**	**VIII. Контроль (анализ) защищенности персональных данных (АНЗ)**					
8	**Приказ 17**	АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
8	**Приказ 21**	АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
8	**Приказ 17**	АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации		+	+	+
8	**Приказ 21**	АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
8	**Приказ 17**	АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
8	**Приказ 21**	АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+

8	**Приказ 17**	АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
8	**Приказ 21**	АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
8	**Приказ 17**	АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе		+	+	+
8	**Приказ 21**	АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+
9	**Приказ 17**	**IX. Обеспечение целостности информационной системы и информации (ОЦЛ)**					
9	**Приказ 21**	**IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ)**					
8	**Приказ 31**	**VIII. Обеспечение целостности (ОЦЛ)**					
8	**Приказ 239**	**VIII. Обеспечение целостности (ОЦЛ)**					
8	**Приказ 31**	ОЦЛ.0	Разработка политики обеспечения целостности		+	+	+
8	**Приказ 239**	ОЦЛ.0	Регламентация правил и процедур обеспечения целостности		+	+	+
9	**Приказ 17**	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
9	**Приказ 21**	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
8	**Приказ 31**	ОЦЛ.1	Контроль целостности программного обеспечения		+	+	+
8	**Приказ 239**	ОЦЛ.1	Контроль целостности программного обеспечения		+	+	+
9	**Приказ 17**	ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы				
9	**Приказ 21**	ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
8	**Приказ 31**	ОЦЛ.2	Контроль целостности информации				
8	**Приказ 239**	ОЦЛ.2	Контроль целостности информации				
9	**Приказ 17**	ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций		+	+	+
9	**Приказ 21**	ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
8	**Приказ 31**	ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему				+
8	**Приказ 239**	ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему				+
9	**Приказ 17**	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)			+	+
9	**Приказ 21**	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)			+	+
8	**Приказ 31**	ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему			+	+
8	**Приказ 239**	ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему			+	+
9	**Приказ 17**	ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				
9	**Приказ 21**	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),методов), и исключение неправомерной передачи информации из информационной системы				
8	**Приказ 31**	ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях			+	+
8	**Приказ 239**	ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях			+	+
9	**Приказ 17**	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				+
9	**Приказ 21**	ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
8	**Приказ 31**	ОЦЛ.6	Обезличивание и (или) деидентификация информации				
8	**Приказ 239**	ОЦЛ.6	Обезличивание и (или) деидентификация информации				
9	**Приказ 17**	ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
9	**Приказ 21**	ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				

9	**Приказ 17**	ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях				
9	**Приказ 21**	ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
10	**Приказ 17**	**X. Обеспечение доступности информации (ОДТ)**					
10	**Приказ 21**	**X. Обеспечение доступности персональных данных (ОДТ)**					
9	**Приказ 31**	**IX. Обеспечение доступности (ОДТ)**					
9	**Приказ 239**	**IX. Обеспечение доступности (ОДТ)**					
9	**Приказ 31**	ОДТ.0	Разработка политики обеспечения доступности		+	+	+
9	**Приказ 239**	ОДТ.0	Регламентация правил и процедур обеспечения доступности		+	+	+
10	**Приказ 17**	ОДТ.1	Использование отказоустойчивых технических средств				+
10	**Приказ 21**	ОДТ.1	Использование отказоустойчивых технических средств				
9	**Приказ 31**	ОДТ.1	Использование отказоустойчивых технических средств			+	+
9	**Приказ 239**	ОДТ.1	Использование отказоустойчивых технических средств			+	+
10	**Приказ 17**	ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				+
10	**Приказ 21**	ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
9	**Приказ 31**	ОДТ.2	Резервирование средств и систем			+	+
9	**Приказ 239**	ОДТ.2	Резервирование средств и систем			+	+
10	**Приказ 17**	ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование			+	+
10	**Приказ 21**	ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
9	**Приказ 31**	ОДТ.3	Контроль безотказного функционирования средств и систем			+	+
9	**Приказ 239**	ОДТ.3	Контроль безотказного функционирования средств и систем			+	+
10	**Приказ 17**	ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации			+	+
10	**Приказ 21**	ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
9	**Приказ 31**	ОДТ.4	Резервное копирование информации		+	+	+
9	**Приказ 239**	ОДТ.4	Резервное копирование информации		+	+	+
10	**Приказ 17**	ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течении установленного временного интервала			+	+
10	**Приказ 21**	ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
9	**Приказ 31**	ОДТ.5	Обеспечение возможности восстановления информации		+	+	+
9	**Приказ 239**	ОДТ.5	Обеспечение возможности восстановления информации		+	+	+
10	**Приказ 17**	ОДТ.6	Кластеризация информационной системы и (или) ее сегментов				
9	**Приказ 31**	ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях		+	+	+
9	**Приказ 239**	ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях		+	+	+
10	**Приказ 17**	ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации			+	+
9	**Приказ 31**	ОДТ.7	Кластеризация информационной (автоматизированной) системы				
9	**Приказ 239**	ОДТ.7	Кластеризация информационной (автоматизированной) системы				
9	**Приказ 31**	ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи		+	+	+
9	**Приказ 239**	ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи		+	+	+
12	**Приказ 17**	**XII. Защита технических средств (ЗТС)**					
12	**Приказ 21**	**XII. Защита технических средств (ЗТС)**					
10	**Приказ 31**	**X. Защита технических средств и систем (ЗТС)**					
10	**Приказ 239**	**X. Защита технических средств и систем (ЗТС)**					
10	**Приказ 31**	ЗТС.0	Разработка политики защиты технических средств и систем		+	+	+
10	**Приказ 239**	ЗТС.0	Регламентация правил и процедур защиты технических средств и систем		+	+	+
12	**Приказ 17**	ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				

12	**Приказ 21**	ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
10	**Приказ 31**	ЗТС.1	Защита информации от утечки по техническим каналам				
10	**Приказ 239**	ЗТС.1	Защита информации от утечки по техническим каналам				
12	**Приказ 17**	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования		+	+	+
12	**Приказ 21**	ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
10	**Приказ 31**	ЗТС.2	Организация контролируемой зоны		+	+	+
10	**Приказ 239**	ЗТС.2	Организация контролируемой зоны		+	+	+
12	**Приказ 17**	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 и помещения и сооружения, в которых они установлены		+	+	+
12	**Приказ 21**	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	+	+	+	+
10	**Приказ 31**	ЗТС.3	Управление физическим доступом		+	+	+
10	**Приказ 239**	ЗТС.3	Управление физическим доступом		+	+	+
12	**Приказ 17**	ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр		+	+	+
12	**Приказ 21**	ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
10	**Приказ 31**	ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр		+	+	+
10	**Приказ 239**	ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр		+	+	+
12	**Приказ 17**	ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				+
12	**Приказ 21**	ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
10	**Приказ 31**	ЗТС.5	Защита от внешних воздействий		+	+	+
10	**Приказ 239**	ЗТС.5	Защита от внешних воздействий		+	+	+
10	**Приказ 31**	ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации				
10	**Приказ 239**	ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации				
13	**Приказ 17**	**XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)**					
13	**Приказ 21**	**XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)**					
11	**Приказ 31**	**XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)**					
11	**Приказ 239**	**XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)**					
11	**Приказ 31**	ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов		+	+	+
11	**Приказ 239**	ЗИС.0	Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов		+	+	+
13	**Приказ 17**	ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы			+	+
13	**Приказ 21**	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				+
11	**Приказ 31**	ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями		+	+	+
11	**Приказ 239**	ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями		+	+	+
13	**Приказ 17**	ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
13	**Приказ 21**	ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				

11	**Приказ 31**	ЗИС.2	Защита периметра информационной (автоматизированной) системы		+	+	+
11	**Приказ 239**	ЗИС.2	Защита периметра информационной (автоматизированной) системы		+	+	+
13	**Приказ 17**	ЗИС.3	Обеспечение защиты информации 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		+	+	+
13	**Приказ 21**	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	+	+	+	+
11	**Приказ 31**	ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы		+	+	+
11	**Приказ 239**	ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы		+	+	+
13	**Приказ 17**	ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
13	**Приказ 21**	ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
11	**Приказ 31**	ЗИС.4	Сегментирование информационной (автоматизированной) системы			+	+
11	**Приказ 239**	ЗИС.4	Сегментирование информационной (автоматизированной) системы			+	+
13	**Приказ 17**	ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств		+	+	+
13	**Приказ 21**	ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
11	**Приказ 31**	ЗИС.5	Организация демилитаризованной зоны		+	+	+
11	**Приказ 239**	ЗИС.5	Организация демилитаризованной зоны		+	+	+
13	**Приказ 17**	ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами				
13	**Приказ 21**	ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
11	**Приказ 31**	ЗИС.6	Управление сетевыми потоками				
11	**Приказ 239**	ЗИС.6	Управление сетевыми потоками		+	+	+
13	**Приказ 17**	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			+	+
13	**Приказ 21**	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				
11	**Приказ 31**	ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")				
11	**Приказ 239**	ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")				
13	**Приказ 17**	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			+	+
13	**Приказ 21**	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				
11	**Приказ 31**	ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы		+	+	+
11	**Приказ 239**	ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы		+	+	+
13	**Приказ 17**	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			+	+
13	**Приказ 21**	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				
11	**Приказ 31**	ЗИС.9	Создание гетерогенной среды				
11	**Приказ 239**	ЗИС.9	Создание гетерогенной среды				

13	**Приказ 17**	ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
13	**Приказ 21**	ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
11	**Приказ 31**	ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем				
11	**Приказ 239**	ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем				
13	**Приказ 17**	ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
13	**Приказ 21**	ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
11	**Приказ 31**	ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
11	**Приказ 239**	ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
13	**Приказ 17**	ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю			+	+
13	**Приказ 21**	ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
11	**Приказ 31**	ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти				
11	**Приказ 239**	ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти				
13	**Приказ 17**	ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя			+	+
13	**Приказ 21**	ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
11	**Приказ 31**	ЗИС.13	Защита неизменяемых данных			+	+
11	**Приказ 239**	ЗИС.13	Защита неизменяемых данных			+	+
13	**Приказ 17**	ЗИС.14	Использование устройств терминального доступа для обработки информации				
13	**Приказ 21**	ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
11	**Приказ 31**	ЗИС.14	Использование неперезаписываемых машинных носителей информации				
11	**Приказ 239**	ЗИС.14	Использование неперезаписываемых машинных носителей информации				
13	**Приказ 17**	ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации			+	+
13	**Приказ 21**	ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
11	**Приказ 31**	ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек				
11	**Приказ 239**	ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек				
13	**Приказ 17**	ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов				
13	**Приказ 21**	ЗИС.16	Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
11	**Приказ 31**	ЗИС.16	Защита от спама			+	+
11	**Приказ 239**	ЗИС.16	Защита от спама			+	+
13	**Приказ 17**	ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
13	**Приказ 21**	ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
11	**Приказ 31**	ЗИС.17	Защита информации от утечек				
11	**Приказ 239**	ЗИС.17	Защита информации от утечек				
13	**Приказ 17**	ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения				
13	**Приказ 21**	ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
11	**Приказ 31**	ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию				

11	**Приказ 239**	ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию				
13	**Приказ 17**	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
13	**Приказ 21**	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
11	**Приказ 31**	ЗИС.19	Защита информации при ее передаче по каналам связи		+	+	+
11	**Приказ 239**	ЗИС.19	Защита информации при ее передаче по каналам связи		+	+	+
13	**Приказ 17**	ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
13	**Приказ 21**	ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
11	**Приказ 31**	ЗИС.20	Обеспечение доверенных канала, маршрута		+	+	+
11	**Приказ 239**	ЗИС.20	Обеспечение доверенных канала, маршрута		+	+	+
13	**Приказ 17**	ЗИС.21	Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы				+
11	**Приказ 31**	ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств		+	+	+
11	**Приказ 239**	ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств		+	+	+
13	**Приказ 17**	ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы			+	+
11	**Приказ 31**	ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами				
11	**Приказ 239**	ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами				
13	**Приказ 17**	ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями			+	+
11	**Приказ 31**	ЗИС.23	Контроль использования мобильного кода			+	+
11	**Приказ 239**	ЗИС.23	Контроль использования мобильного кода				
13	**Приказ 17**	ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения			+	+
11	**Приказ 31**	ЗИС.24	Контроль передачи речевой информации			+	+
11	**Приказ 239**	ЗИС.24	Контроль передачи речевой информации				
13	**Приказ 17**	ЗИС.25	Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)				
11	**Приказ 31**	ЗИС.25	Контроль передачи видеоинформации			+	+
11	**Приказ 239**	ЗИС.25	Контроль передачи видеоинформации				
13	**Приказ 17**	ЗИС.26	Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем				
11	**Приказ 31**	ЗИС.26	Подтверждение происхождения источника информации				
11	**Приказ 239**	ЗИС.26	Подтверждение происхождения источника информации				
13	**Приказ 17**	ЗИС.27	Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации				
11	**Приказ 31**	ЗИС.27	Обеспечение подлинности сетевых соединений			+	+
11	**Приказ 239**	ЗИС.27	Обеспечение подлинности сетевых соединений			+	+
13	**Приказ 17**	ЗИС.28	Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы				
11	**Приказ 31**	ЗИС.28	Исключение возможности отрицания отправки информации			+	+
11	**Приказ 239**	ЗИС.28	Исключение возможности отрицания отправки информации				
13	**Приказ 17**	ЗИС.29	Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы				
11	**Приказ 31**	ЗИС.29	Исключение возможности отрицания получения информации			+	+
11	**Приказ 239**	ЗИС.29	Исключение возможности отрицания получения информации				
13	**Приказ 17**	ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе		+	+	+
11	**Приказ 31**	ЗИС.30	Использование устройств терминального доступа				
11	**Приказ 239**	ЗИС.30	Использование устройств терминального доступа				
11	**Приказ 31**	ЗИС.31	Защита от скрытых каналов передачи информации				+
11	**Приказ 239**	ЗИС.31	Защита от скрытых каналов передачи информации				

11	**Приказ 31**	ЗИС.32	Защита беспроводных соединений		+	+	+
11	**Приказ 239**	ЗИС.32	Защита беспроводных соединений		+	+	+
11	**Приказ 31**	ЗИС.33	Исключение доступа через общие ресурсы				+
11	**Приказ 239**	ЗИС.33	Исключение доступа через общие ресурсы				+
11	**Приказ 31**	ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)		+	+	+
11	**Приказ 239**	ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)		+	+	+
11	**Приказ 31**	ЗИС.35	Управление сетевыми соединениями			+	+
11	**Приказ 239**	ЗИС.35	Управление сетевыми соединениями		+	+	+
11	**Приказ 31**	ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем				
11	**Приказ 239**	ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем				
11	**Приказ 31**	ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)				
11	**Приказ 239**	ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)				
11	**Приказ 31**	ЗИС.38	Защита информации при использовании мобильных устройств		+	+	+
11	**Приказ 239**	ЗИС.38	Защита информации при использовании мобильных устройств		+	+	+
11	**Приказ 31**	ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных		+	+	+
11	**Приказ 239**	ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных		+	+	+
11	**Приказ 17**	**XI. Защита среды виртуализации (ЗСВ)**					
11	**Приказ 21**	**XI. Защита среды виртуализации (ЗСВ)**					
11	**Приказ 17**	ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации		+	+	+
11	**Приказ 21**	ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
11	**Приказ 17**	ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин		+	+	+
11	**Приказ 21**	ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
11	**Приказ 17**	ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
11	**Приказ 21**	ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
11	**Приказ 17**	ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры			+	+
11	**Приказ 21**	ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
11	**Приказ 17**	ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
11	**Приказ 21**	ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
11	**Приказ 17**	ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
11	**Приказ 21**	ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
11	**Приказ 17**	ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
11	**Приказ 21**	ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
11	**Приказ 17**	ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
11	**Приказ 21**	ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
11	**Приказ 17**	ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
11	**Приказ 21**	ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
11	**Приказ 17**	ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей		+	+	+

11	**Приказ 21**	ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
14	**Приказ 21**	**XIV. Выявление инцидентов и реагирование на них (ИНЦ)**					
12	**Приказ 31**	**XII. Реагирование на компьютерные инциденты (ИНЦ)**					
12	**Приказ 239**	**XII. Реагирование на компьютерные инциденты (ИНЦ)**					
12	**Приказ 31**	ИНЦ.0	Разработка политики реагирования на компьютерные инциденты		+	+	+
12	**Приказ 239**	ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты		+	+	+
14	**Приказ 21**	ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
12	**Приказ 31**	ИНЦ.1	Выявление компьютерных инцидентов		+	+	+
12	**Приказ 239**	ИНЦ.1	Выявление компьютерных инцидентов		+	+	+
14	**Приказ 21**	ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
12	**Приказ 31**	ИНЦ.2	Информирование о компьютерных инцидентах		+	+	+
12	**Приказ 239**	ИНЦ.2	Информирование о компьютерных инцидентах		+	+	+
14	**Приказ 21**	ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
12	**Приказ 31**	ИНЦ.3	Анализ компьютерных инцидентов		+	+	+
12	**Приказ 239**	ИНЦ.3	Анализ компьютерных инцидентов		+	+	+
14	**Приказ 21**	ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
12	**Приказ 31**	ИНЦ.4	Устранение последствий компьютерных инцидентов		+	+	+
12	**Приказ 239**	ИНЦ.4	Устранение последствий компьютерных инцидентов		+	+	+
14	**Приказ 21**	ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+
12	**Приказ 31**	ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов		+	+	+
12	**Приказ 239**	ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов		+	+	+
14	**Приказ 21**	ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
12	**Приказ 31**	ИНЦ.6	Хранение и защита информации о компьютерных инцидентах				+
12	**Приказ 239**	ИНЦ.6	Хранение и защита информации о компьютерных инцидентах		+	+	+
15	**Приказ 21**	**XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)**					
13	**Приказ 31**	**XIII. Управление конфигурацией (УКФ)**					
13	**Приказ 239**	**XIII. Управление конфигурацией (УКФ)**					
13	**Приказ 31**	УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы		+	+	+
13	**Приказ 239**	УКФ.0	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы		+	+	+
15	**Приказ 21**	УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
13	**Приказ 31**	УКФ.1	Идентификация объектов управления конфигурацией				
13	**Приказ 239**	УКФ.1	Идентификация объектов управления конфигурацией				
15	**Приказ 21**	УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
13	**Приказ 31**	УКФ.2	Управление изменениями		+	+	+
13	**Приказ 239**	УКФ.2	Управление изменениями		+	+	+
15	**Приказ 21**	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		+	+	+
13	**Приказ 31**	УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения		+	+	+
13	**Приказ 239**	УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения		+	+	+
15	**Приказ 21**	УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+
13	**Приказ 31**	УКФ.4	Контроль действий по внесению изменений				
13	**Приказ 239**	УКФ.4	Контроль действий по внесению изменений				
14	**Приказ 31**	**XIV. Управление обновлениями программного обеспечения (ОПО)**					

14	Приказ 239	**XIV. Управление обновлениями программного обеспечения (ОПО)**					
14	Приказ 31	ОПО.0	Разработка политики управления обновлениями программного обеспечения		+	+	+
14	Приказ 239	ОПО.0	Регламентация правил и процедур управления обновлениями программного обеспечения		+	+	+
14	Приказ 31	ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника		+	+	+
14	Приказ 239	ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника		+	+	+
14	Приказ 31	ОПО.2	Контроль целостности обновлений программного обеспечения		+	+	+
14	Приказ 239	ОПО.2	Контроль целостности обновлений программного обеспечения		+	+	+
14	Приказ 31	ОПО.3	Тестирование обновлений программного обеспечения		+	+	+
14	Приказ 239	ОПО.3	Тестирование обновлений программного обеспечения		+	+	+
14	Приказ 31	ОПО.4	Установка обновлений программного обеспечения		+	+	+
14	Приказ 239	ОПО.4	Установка обновлений программного обеспечения		+	+	+
15	Приказ 31	**XV. Планирование мероприятий по обеспечению безопасности (ПЛН)**					
15	Приказ 239	**XV. Планирование мероприятий по обеспечению безопасности (ПЛН)**					
15	Приказ 31	ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации		+	+	+
15	Приказ 239	ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации		+	+	+
15	Приказ 31	ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации		+	+	+
15	Приказ 239	ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации		+	+	+
15	Приказ 31	ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации		+	+	+
15	Приказ 239	ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации		+	+	+
16	Приказ 31	**XVI. Обеспечение действий в нештатных ситуациях (ДНС)**					
16	Приказ 239	**XVI. Обеспечение действий в нештатных ситуациях (ДНС)**					
16	Приказ 31	ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях		+	+	+
16	Приказ 239	ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях		+	+	+
16	Приказ 31	ДНС.1	Разработка плана действий в нештатных ситуациях		+	+	+
16	Приказ 239	ДНС.1	Разработка плана действий в нештатных ситуациях		+	+	+
16	Приказ 31	ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях		+	+	+
16	Приказ 239	ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях		+	+	+
16	Приказ 31	ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций			+	+
16	Приказ 239	ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций			+	+
16	Приказ 31	ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций			+	+
16	Приказ 239	ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций			+	+
16	Приказ 31	ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций		+	+	+
16	Приказ 239	ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций		+		+
16	Приказ 31	ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения		+	+	+
16	Приказ 239	ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения		+	+	+
17	Приказ 31	**XVII. Информирование и обучение персонала (ИПО)**					
17	Приказ 239	**XVII. Информирование и обучение персонала (ИПО)**					
17	Приказ 31	ИПО.0	Разработка политики информирования и обучения персонала		+	+	+
17	Приказ 239	ИПО.0	Регламентация правил и процедур информирования и обучения персонала		+	+	+
17	Приказ 31	ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы		+	+	+
17	Приказ 239	ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы		+	+	+
17	Приказ 31	ИПО.2	Обучение персонала правилам безопасной работы		+	+	+
17	Приказ 239	ИПО.2	Обучение персонала правилам безопасной работы		+	+	+
17	Приказ 31	ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы			+	+
17	Приказ 239	ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы			+	+

17	**Приказ 31**	ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы		+	+	+
17	**Приказ 239**	ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы		+	+	+