Методические рекомендации
по обеспечению информационной безопасности вещателей телерадиоканалов, имеющих соответствующие лицензии

1. Настоящие Методические рекомендации по обеспечению информационной безопасности информационных ресурсов вещателей телерадиоканалов, имеющих соответствующие лицензии (далее – Рекомендации) определяют перечень комплексных мер, которые рекомендуется реализовать вещателям телерадиоканалов, имеющих соответствующие лицензии (далее – Организации) в целях обеспечения информационной безопасности своих информационных ресурсов.

2. В целях реализации комплексных мер по обеспечению информационной безопасности информационных ресурсов Организаций рекомендуется:

2.1. В течение 30 рабочих дней с момента получения настоящих Рекомендаций определить информационные ресурсы, подлежащие защите от несанкционированного доступа и компьютерных атак и составить перечни соответствующих информационных ресурсов.

2.2. Разработать комплексную систему защиты информации.

В течение четырех месяцев с момента определения информационных ресурсов, подлежащих защите, Организациям рекомендуется разработать и согласовать с ФСТЭК России и ФСБ России в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации, модели угроз и нарушителя безопасности информации (далее – МуиН) и определить необходимые меры по защите информации.

При разработке МуиН рекомендуется руководствоваться нормативными требованиями и методическими рекомендациями, установленными ФСТЭК России, а также учитывать объекты защиты, приведенные в Приложении № 1 к Рекомендациям.

В течение трех месяцев с момента утверждения МуиН Организациям рекомендуется разработать комплексную систему защиты информации (далее – КСЗИ) и дорожную карту создания и развития КСЗИ (далее – дорожная карта), учитывающие необходимость использования сертифицированных на соответствие требованиям по безопасности информации средств защиты информации
или средств, прошедших оценку соответствия в форме испытаний или приемки.

Реализацию организационных и технических мер по обеспечению информационной безопасности рекомендуется осуществлять с учетом МуиН. При этом они не должны оказывать негативного влияния на функционирование объектов защиты.

Рекомендованный базовый состав мер по обеспечению безопасности информационных ресурсов определен в Приложении № 2 к Рекомендациям. Указанный набор мер не является исчерпывающим и может быть дополнен (скорректирован) с учетом актуальных угроз безопасности информации.

Утвержденные Организациями МуиН и КСЗИ не позднее одного месяца с момента их утверждения необходимо направить в Минцифры России, ФСБ России и ФСТЭК России.

2.3. Провести оценку защищенности информационных ресурсов и устранить выявленные недостатки.

Организациям на регулярной основе, но не реже одного раза в год, рекомендуется проводить оценку защищенности информационных ресурсов, подлежащих защите, с привлечением организаций, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации или имеющих соглашение о сотрудничестве (взаимодействие) в области обнаружения, предупреждения и ликвидации последствий компьютерных атак с Национальным координационным центром по компьютерным инцидентам или ФСБ России и имеющих лицензию на деятельность по технической защите конфиденциальной информации и ее модификации в средствах и системах информатизации.

В ходе оценки защищенности информационных ресурсов от компьютерных атак рекомендуется проводить оценку реализации мер по обеспечению безопасности, в том числе выявлять возможные точки проникновения внешнего нарушителя в информационные ресурсы (каналы удаленного доступа, точки подключения к сети «Интернет», точки взаимодействия с иными информационными (автоматизированными) системами, беспроводные сети передачи данных и другие способы), и анализ уязвимостей возможных точек проникновения внешнего нарушителя, включающий контроль состава и уязвимость установленного программного обеспечения, в том числе прикладного и системного программного обеспечения.

По итогу проведенной оценки защищенности Организациям рекомендуется разработать план мероприятий по устранению выявленных уязвимостей информационных ресурсов и в течение 10 рабочих дней направить его, а также информацию по исполнению плана в Минцифры России.

2.4. Принимать дополнительные меры по повышению уровня защищенности информационных ресурсов.

ФСТЭК России, 8 Центр ФСБ России, Минцифры России и Роскомнадзор (в случае выявления угроз, связанных с подменой информации на интернет-ресурсах и массового распространения заведомо ложных сообщений) с учетом меняющихся угроз в информационной сфере в пределах своей компетенции могут направлять Организациям перечень рекомендованных первоочередных и дополнительных организационных и технических мер, необходимых для повышения защищенности информационных ресурсов.

С целью нивелирования угроз информационной безопасности Организациям при получении такого перечня рекомендуется в возможно короткий срок или в обозначенные направившим органом сроки предоставить в его адрес информацию об исполнении указанных организационных и технических мер.

С целью повышения уровня информационной безопасности Минцифры России по согласованию с 8 Центром ФСБ России и с привлечением организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации и ее модификации в средствах и системах информатизации, рекомендуется на постоянной основе в рамках заключенных с Организациями соглашений принимает дополнительные меры по повышению защищенности, определяемых соглашениями, в том числе мероприятий по контролю внешнего периметра, зрелости уровня информационной безопасности и выявлению признаков компрометации информационных ресурсов Организаций.

Приложение № 1
к Методическим
рекомендациям

Рекомендуемый перечень объектов защиты

а) в информационных системах:

- информация, обрабатываемая в информационной системе;
- программно-аппаратные средства (в том числе машинные носители информации, автоматизированные рабочие места, серверы, телекоммуникационное оборудование, линии связи, средства обработки буквенно-цифровой, графической, видео- и речевой информации);
- программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);
- средства защиты информации;
- архитектура и конфигурация информационной системы;

б) в информационно-телекоммуникационных сетях:

- информация, передаваемая по линиям связи;
- телекоммуникационное оборудование (в том числе программное обеспечение, система управления);
- средства защиты информации;
- архитектура и конфигурация информационно-телекоммуникационной сети;

в) в автоматизированных системах управления:

- информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая информация);
- программно-аппаратные средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, линии связи, программируемые логические контролеры, производственное, технологическое оборудование (исполнительные устройства);
- программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);
- средства защиты информации;
- архитектура и конфигурация автоматизированной системы управления.

Приложение № 2
к Методическим
рекомендациям

Рекомендуемый состав мер по обеспечению безопасности информационным ресурсам российских средств массовой информации

№ п/п	Меры обеспечения безопасности
1.	Разработка политики идентификации и аутентификации
2.	Идентификация и аутентификация пользователей и инициируемых ими процессов
3.	Идентификация и аутентификация устройств
4	Управление идентификаторами
5	Управление средствами аутентификации
6	Идентификация и аутентификация внешних пользователей
7	Защита аутентификационной информации при передаче
8	Разработка политики управления доступом
9	Управление учетными записями пользователей
10	Реализация политик управления доступом
11	Разделение полномочий (ролей) пользователей
12	Назначение минимально необходимых прав и привилегий
13	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему
14	Блокирование сеанса доступа пользователя при неактивности
15	Управление действиями пользователей до идентификации и аутентификации
16	Реализация защищенного удаленного доступа
17	Контроль доступа из внешних информационных (автоматизированных) систем
18	Разработка политики защиты машинных носителей информации
19	Учет машинных носителей информации
20	Управление физическим доступом к машинным носителям информации
21	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
22	Контроль подключения машинных носителей информации
23	Уничтожение (стирание) информации на машинных носителях информации
24	Разработка политики аудита безопасности
25	Инвентаризация информационных ресурсов
26	Анализ уязвимостей и их устранение

27	Генерирование временных меток и (или) синхронизация системного времени
28	Регистрация событий безопасности
29	Защита информации о событиях безопасности
30	Мониторинг безопасности
31	Реагирование на сбои при регистрации событий безопасности
32	Проведение внутренних аудитов
33	Разработка политики антивирусной защиты
34	Реализация антивирусной защиты
35	Антивирусная защита электронной почты и иных сервисов
36	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
37	Разработка политики обеспечения целостности
38	Контроль целостности программного обеспечения
39	Разработка политики обеспечения доступности
40	Резервное копирование информации
41	Обеспечение возможности восстановления информации
42	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях
43	Контроль предоставляемых вычислительных ресурсов и каналов связи
44	Выработка политики защиты технических средств и систем
45	Организация контролируемой зоны
46	Управление физическим доступом
47	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
48	Защита от внешних воздействий
49	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов
50	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями
51	Защита периметра информационной (автоматизированной) системы
52	Эшелонированная защита информационной (автоматизированной) системы
53	Организация демилитаризованной зоны
54	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы
55	Защита информации при ее передаче по каналам связи
56	Обеспечение доверенных канала, маршрута
57	Запрет несанкционированной удаленной активации периферийных устройств
58	Защита беспроводных соединений
59	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)
60	Защита информации при использовании мобильных устройств

61	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
62	Разработка политики реагирования на компьютерные инциденты
63	Выявление компьютерных инцидентов
64	Информирование о компьютерных инцидентах
65	Анализ компьютерных инцидентов
66	Устранение последствий компьютерных инцидентов
67	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов
68	Разработка политики управления конфигурацией информационной автоматизированной) системы
69	Управление изменениями
70	Установка (инсталляция) только разрешенного к использованию программного обеспечения
71	Разработка политики управления обновлениями программного обеспечения
72	Поиск, получение обновлений программного обеспечения от доверенного источника
73	Контроль целостности обновлений программного обеспечения
74	Тестирование обновлений программного обеспечения
75	Установка обновлений программного обеспечения
76	Разработка политики планирования мероприятий по обеспечению защиты информации
77	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации
78	Контроль выполнения мероприятий по обеспечению защиты информации
79	Разработка политики обеспечения действий в нештатных ситуациях
80	Разработка плана действий в нештатных ситуациях
81	Обучение и отработка действий персонала в нештатных ситуациях
82	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций
83	Разработка политики информирования и обучения персонала
84	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы
85	Обучение персонала правилам безопасной работы
86	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по перечню первоочередных мер, необходимых для обеспечения информационной безопасности информационных ресурсов средств массовой информации

1. Настоящие Методические рекомендации по перечню первоочередных мер, необходимых для обеспечения информационной безопасности информационных ресурсов средств массовой информации, (далее – Методические рекомендации) определяют перечень комплексных мероприятий, которые рекомендуется реализовать организациям государственных средств массовой информации; вещателям обязательных общедоступных теле- и радиоканалов; вещателям теле- и радиоканалов, осуществляющих эфирное вещание; владельцам аудиовизуальных сервисов, включенных в Реестр аудиовизуальных сервисов; учредителю организации, уполномоченной на обеспечение распространения общероссийских обязательных общедоступных телеканалов и телеканалов, получивших право на осуществление эфирного цифрового наземного вещания с использованием позиций в мультиплексах на всей территории Российской Федерации в информационно-телекоммуникационной сети «Интернет» (ООО «Витрина ТВ»), а также операторам связи, осуществляющим трансляцию теле- и радиоканалов в своих сетях связи (далее – Организации), в целях обеспечения информационной безопасности своих информационных ресурсов.

2. В целях реализации комплексных мероприятий по обеспечению информационной безопасности информационных ресурсов Организаций рекомендуется:

2.1. Определить информационные ресурсы, подлежащие защите от несанкционированного доступа и компьютерных атак.

В течение 20 рабочих дней с момента получения настоящих методических рекомендаций рекомендуется определить информационные ресурсы, подлежащие защите от несанкционированного доступа и компьютерных атак, и направить в Минцифры России в указанный срок перечни соответствующих информационных ресурсов.

Минцифры России в течение 10 рабочих дней с момента получения перечня информационных ресурсов, полученных в соответствии с настоящим пунктом, рекомендуется направить его в 8 Центр ФСБ России и ФСТЭК России.

При наличии замечаний, в том числе полученных от 8 Центр ФСБ России и ФСТЭК России, в течение 20 рабочих дней со дня получения перечня информационных ресурсов Минцифры России рекомендуется направить их Организациям на доработку с указанием причин, послуживших основанием для доработки.

В случае направления соответствующих замечаний Организациям рекомендуется в течение 10 рабочих дней со дня их получения доработать

перечень информационных ресурсов и повторно направить скорректированный перечень в Минцифры России.

В случае изменения перечня информационных ресурсов рекомендуется в течение 10 рабочих дней с момента его изменения рекомендуется Организациям направить в Минцифры России актуализированный перечень информационных ресурсов.

Полученные скорректированные перечни информационных ресурсов рекомендуется в течение 10 рабочих дней со дня их получения Минцифры России направить в 8 Центр ФСБ России и ФСТЭК России.

2.2. Разработать и создать комплексную систему защиты информации.

В течение четырех месяцев с момента определения информационных ресурсов, подлежащих защите, Организациям рекомендуется разработать и согласовать с ФСТЭК России и ФСБ России в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации, модели угроз и нарушителя безопасности информации (далее – МуиН) и определить необходимые меры по защите информации.

При разработке МуиН рекомендуется руководствоваться нормативными требованиями и методическими рекомендациями, установленными ФСТЭК России, а также учитывать объекты защиты, приведенные в Приложении № 1 к Методическим рекомендациям.

Согласованные ФСТЭК России и ФСБ России (при необходимости) и утвержденные Организациями МуиН не позднее одного месяца с момента их утверждения рекомендуется направить в Минцифры России.

В течение трех месяцев с момента утверждения МуиН рекомендуется Организациям разработать комплексную систему защиты информации (далее – КСЗИ) и дорожную карту создания и развития КСЗИ (далее – дорожная карта), учитывающие необходимость использования сертифицированных на соответствие требованиям по безопасности средств защиты информации или средств, прошедших оценку соответствия в форме испытаний или приемки, и, в указанный срок, направить дорожную карту в Минцифры России.

Реализацию организационных и технических мер рекомендуется осуществлять с учетом угроз безопасности информации. При этом они не должны оказывать негативного влияния на функционирование объектов защиты.

Рекомендованный базовый состав мер по обеспечению безопасности информационных ресурсов определен в Приложении № 2 к Методическим рекомендациям. Указанный набор мер не является исчерпывающим и может быть дополнен (скорректирован) с учетом актуальных угроз безопасности информации.

Минцифры России в течение 10 рабочих дней со дня получения от Организаций дорожной карты рекомендуется направить ее в 8 Центр ФСБ России (в случае использования средств криптографической защиты информации (далее – СКЗИ) и ФСТЭК России.

При наличии замечаний, в том числе полученных от 8 Центра ФСБ России и ФСТЭК России, Минцифры России рекомендуется в течение 20 рабочих дней

со дня получения дорожной карты направить их Организациям на доработку с указанием причин, послуживших основанием для доработки.

В случае направления замечаний рекомендуется Организациям в течение 10 рабочих дней со дня их получения доработать дорожную карту и повторно ее направить в Минцифры России.

Полученную скорректированную дорожную карту в течение 10 рабочих дней рекомендуется направить Минцифры России в 8 Центр ФСБ России (в случае использования СКЗИ) и ФСТЭК России.

На ежемесячной основе не позднее 10 числа следующего за отчетным месяцем рекомендуется Организациям предоставлять в Минцифры России актуализированный статус исполнения дорожной карты.

2.3. Провести оценку защищенности информационных ресурсов и устранить выявленные недостатки.

Организациям в соответствии с установленной Минцифры России методикой, согласованной с 8 Центром ФСБ России, на регулярной основе, но не реже одного раза в год, рекомендуется проводить оценку защищенности информационных ресурсов, подлежащих защите, с привлечением организаций, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации или имеющих соглашение о сотрудничестве (взаимодействие) в области обнаружения, предупреждения и ликвидации последствий компьютерных атак с Национальным координационным центром по компьютерным инцидентам или ФСБ России и имеющих лицензию на деятельность по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, и направлять отчет в Минцифры России по форме, определенной Минцифры России, согласованной с 8 Центром ФСБ России.

В ходе оценки защищенности информационных ресурсов от компьютерных атак рекомендуется проводить оценку реализации мер по обеспечению безопасности, в том числе выявлять возможные точки проникновения внешнего нарушителя на информационные ресурсы (каналы удаленного доступа, подключения к сети «Интернет», через взаимодействие с иными информационными (автоматизированными) системами, через беспроводные сети и другие способы) и анализ уязвимостей их узлов, являющимися точками проникновения внешнего нарушителя, включающий контроль состава программного обеспечения, установленного на этих узлах, уязвимостей программного обеспечения узлов, в том числе прикладного и системного программного обеспечения.

Полученные Минцифры России отчеты о проведенной оценке защищенности в течение 10 рабочих дней со дня их получения рекомендуется направлять их в 8 Центр ФСБ России и ФСТЭК России.

Минцифры России при наличии замечаний к отчету о проведенной оценке защищенности, в том числе полученных от 8 Центра ФСБ России и ФСТЭК

России, в течение 20 рабочих дней со дня получения отчета о проведенной оценке защищенности, рекомендуется направлять их Организациям на доработку с указанием причин, послуживших основанием для доработки.

В случае направления замечаний рекомендуется Организациям в течение 10 рабочих дней со дня их получения доработать отчет о проведенной оценке защищенности и повторно направить его в Минцифры России.

Полученный Минцифры России скорректированный отчет о проведенной оценке защищенности рекомендуется в течение 10 рабочих дней со дня его получения направить его в 8 Центр ФСБ России и ФСТЭК России.

По итогу проведенной оценки защищенности и при отсутствии замечаний рекомендуется Организациям сформировать план мероприятий по устранению выявленных уязвимостей информационной безопасности (далее – план) и направить его в Минцифры России по форме, определенной Минцифры России.

В течение 10 рабочих дней со дня получения плана Минцифры России рекомендуется направить его в 8 Центр ФСБ России и ФСТЭК России.

При наличии замечаний к плану, в том числе полученных от 8 Центра ФСБ России и ФСТЭК России, Минцифры России рекомендуется в течение 20 рабочих дней со дня его получения, направить его Организациям на доработку с указанием причин, послуживших основанием для доработки.

В течение 10 рабочих дней со дня поступления замечаний к плану Организациям рекомендуется устранить их и направить доработанный план в Минцифры России.

Полученный скорректированный план в течение 10 рабочих дней со дня получения рекомендуется Минцифры России направить в 8 Центр ФСБ России и ФСТЭК России.

На ежемесячной основе не позднее 10 числа следующего за отчетным месяцем (или в случае внесения изменений в план в течение 5 рабочих дней со дня внесения соответствующих изменений) Организациям рекомендуется направить в Минцифры России отчет о статусе исполнения плана.

После получения отчета о статусе исполнения плана Минцифры России рекомендуется направить его в 8 Центр ФСБ России и ФСТЭК России.

2.4. Принимать дополнительные меры повышения защищенности информационных ресурсов.

ФСТЭК России, 8 Центр ФСБ России, Минцифры России и Роскомнадзор (в случае выявления угроз, связанных с подменой информации на интернет-ресурсах и массового распространения заведомой ложных сообщений) с учетом меняющихся угроз в информационной сфере в пределах своей компетенции могут направлять Организациям перечень рекомендованных первоочередных и дополнительных организационных и технических мер, необходимых для повышения защищенности информационных ресурсов.

С целью нивелирования выявленных угроз Организациям рекомендуется в возможно короткий срок или в обозначенные направившим органом сроки предоставить в его адрес информацию об исполнении указанных организационных и технических мер.

С целью повышения уровня информационной безопасности Организациям рекомендуется Минцифры России по согласованию с 8 Центром ФСБ России с привлечением организаций, имеющих лицензию на деятельность по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, на постоянной основе в рамках заключенных с Организациями соглашений проводить мероприятия по дополнительным мерам повышения защищенности, определяемых соглашением, в том числе мероприятий по контролю внешнего периметра, зрелости уровня информационной безопасности и выявлению признаков компрометации информационных систем.

3. Мониторинг реализации мер по обеспечению информационной безопасности Организаций.

С целью обеспечения мониторинга реализации рекомендуемых мер по обеспечению информационной безопасности Организаций 8 Центр ФСБ России на регулярной основе осуществляет:

мониторинг защищенности доступных из сети Интернет информационных ресурсов Организаций ;

проверку реализуемых рекомендуемых мероприятий по повышению защищенности информационных ресурсов Организаций.

В случае выявления недостатков в обеспечении информационной безопасности 8 Центр ФСБ России подготавливает и направляет результаты мониторинга защищенности, а также рекомендации по повышению уровня защищенности информационных ресурсов Организаций с одновременным направлением копии в Минцифры России.

Минцифры России на основе проводимых мероприятий, рекомендуемых к проведению в рамках настоящих методических рекомендаций, ежемесячно формирует отчет о текущем уровне защищенности Организаций и направляет его в 8 Центр ФСБ России и ФСТЭК России.

Приложение № 1
к Методическим
рекомендациям

Рекомендуемый перечень объектов защиты

а) в информационных системах:
- информация, обрабатываемая в информационной системе;
- программно-аппаратные средства (в том числе машинные носители информации, автоматизированные рабочие места, серверы, телекоммуникационное оборудование, линии связи, средства обработки буквенно-цифровой, графической, видео- и речевой информации);
- программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);
- средства защиты информации;
- архитектура и конфигурация информационной системы;

б) в информационно-телекоммуникационных сетях:
- информация, передаваемая по линиям связи;
- телекоммуникационное оборудование (в том числе программное обеспечение, система управления);
- средства защиты информации;
- архитектура и конфигурация информационно-телекоммуникационной сети;

в) в автоматизированных системах управления:
- информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая информация);
- программно-аппаратные средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, линии связи, программируемые логические контролеры, производственное, технологическое оборудование (исполнительные устройства);
- программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);
- средства защиты информации;
- архитектура и конфигурация автоматизированной системы управления.

Приложение № 2
к Методическим
рекомендациям

Рекомендуемый состав мер по обеспечению безопасности информационным ресурсам российских средств массовой информации

№ п/п	Меры обеспечения безопасности
1.	Разработка политики идентификации и аутентификации
2.	Идентификация и аутентификация пользователей и инициируемых ими процессов
3.	Идентификация и аутентификация устройств
4	Управление идентификаторами
5	Управление средствами аутентификации
6	Идентификация и аутентификация внешних пользователей
7	Защита аутентификационной информации при передаче
8	Разработка политики управления доступом
9	Управление учетными записями пользователей
10	Реализация политик управления доступом
11	Разделение полномочий (ролей) пользователей
12	Назначение минимально необходимых прав и привилегий
13	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему
14	Блокирование сеанса доступа пользователя при неактивности
15	Управление действиями пользователей до идентификации и аутентификации
16	Реализация защищенного удаленного доступа
17	Контроль доступа из внешних информационных (автоматизированных) систем
18	Разработка политики защиты машинных носителей информации
19	Учет машинных носителей информации
20	Управление физическим доступом к машинным носителям информации
21	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
22	Контроль подключения машинных носителей информации
23	Уничтожение (стирание) информации на машинных носителях информации
24	Разработка политики аудита безопасности
25	Инвентаризация информационных ресурсов
26	Анализ уязвимостей и их устранение

27	Генерирование временных меток и (или) синхронизация системного времени
28	Регистрация событий безопасности
29	Защита информации о событиях безопасности
30	Мониторинг безопасности
31	Реагирование на сбои при регистрации событий безопасности
32	Проведение внутренних аудитов
33	Разработка политики антивирусной защиты
34	Реализация антивирусной защиты
35	Антивирусная защита электронной почты и иных сервисов
36	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
37	Разработка политики обеспечения целостности
38	Контроль целостности программного обеспечения
39	Разработка политики обеспечения доступности
40	Резервное копирование информации
41	Обеспечение возможности восстановления информации
42	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях
43	Контроль предоставляемых вычислительных ресурсов и каналов связи
44	Выработка политики защиты технических средств и систем
45	Организация контролируемой зоны
46	Управление физическим доступом
47	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
48	Защита от внешних воздействий
49	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов
50	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями
51	Защита периметра информационной (автоматизированной) системы
52	Эшелонированная защита информационной (автоматизированной) системы
53	Организация демилитаризованной зоны
54	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы
55	Защита информации при ее передаче по каналам связи
56	Обеспечение доверенных канала, маршрута
57	Запрет несанкционированной удаленной активации периферийных устройств
58	Защита беспроводных соединений
59	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)
60	Защита информации при использовании мобильных устройств

61	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
62	Разработка политики реагирования на компьютерные инциденты
63	Выявление компьютерных инцидентов
64	Информирование о компьютерных инцидентах
65	Анализ компьютерных инцидентов
66	Устранение последствий компьютерных инцидентов
67	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов
68	Разработка политики управления конфигурацией информационной автоматизированной) системы
69	Управление изменениями
70	Установка (инсталляция) только разрешенного к использованию программного обеспечения
71	Разработка политики управления обновлениями программного обеспечения
72	Поиск, получение обновлений программного обеспечения от доверенного источника
73	Контроль целостности обновлений программного обеспечения
74	Тестирование обновлений программного обеспечения
75	Установка обновлений программного обеспечения
76	Разработка политики планирования мероприятий по обеспечению защиты информации
77	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации
78	Контроль выполнения мероприятий по обеспечению защиты информации
79	Разработка политики обеспечения действий в нештатных ситуациях
80	Разработка плана действий в нештатных ситуациях
81	Обучение и отработка действий персонала в нештатных ситуациях
82	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций
83	Разработка политики информирования и обучения персонала
84	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы
85	Обучение персонала правилам безопасной работы
86	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы