ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ЦИФРЛЫҚ ДАМУ, ИННОВАЦИЯЛАР ЖӘНЕ АЭРОҒАРЫШ ӨНЕРКӘСІБІ МИНИСТРЛІГІ “МЕМЛЕКЕТТІК РАДИОЖИІЛІК ҚЫЗМЕТІ” ШАРУАШЫЛЫҚ ЖҮРГІЗУ ҚҰҚЫҒЫНДАҒЫ РЕСПУБЛИКАЛЫҚ МЕМЛЕКЕТТІК КӘСІПОРНЫ

РЕСПУБЛИКАНСКОЕ ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ НА ПРАВЕ ХОЗЯЙСТВЕННОГО ВЕДЕНИЯ “ГОСУДАРСТВЕННАЯ РАДИОЧАСТОТНАЯ СЛУЖБА” МИНИСТЕРСТВА ЦИФРОВОГО РАЗВИТИЯ, ИННОВАЦИЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН

БҰЙРЫҚ

_____№_____

ПРИКАЗ

_____№_____

«МРҚ» РМК ақпараттық қауіпсіздік жөніндегі құжаттарын бекіту туралы

Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің «Мемлекеттік радиожиілік қызметі» шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнында (бұдан әрі – «МРҚ» РМК) Қазақстан Республикасының заңнамасымен белгіленген ақпараттық қауіпсіздік талаптарының сақталуын қамтамасыз ету мақсатында, **БҰЙЫРАМЫН:**

1. «МРҚ» РМК ақпараттық қауіпсіздік жөніндегі құжаттары осы бұйрықтың қосымшасына сәйкес бекітілсін.
2. Осы бұйрықтың орындалуын бақылауды өзіме қалдырамын.
3. Осы бұйрық қол қойылған күнінен бастап күшіне енеді және танысуға жатады.

Директор **Р. Нуршабеков**

Орынд.: Сатыбалдиев Қ.
Тел.: 57-55-64

Об утверждении документов по информационной безопасности РГП «ГРС»

С целью обеспечения соблюдения требований информационной безопасности в республиканском государственном предприятии на праве хозяйственного ведения «Государственная радиочастотная служба» Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (далее - РГП «ГРС») установленных законодательством Республики Казахстан **ПРИКАЗЫВАЮ:**

1. Утвердить документы по информационной безопасности РГП «ГРС» согласно приложению к настоящему приказу.
2. Контроль за исполнением настоящего приказа оставляю за собой.
3. Настоящий приказ вступает в силу со дня его подписания и подлежит ознакомлению.

Директор **Р. Нуршабеков**

Исп.: Сатыбалдиев Қ.
Тел.: 57-55-64

ПРИЛОЖЕНИЕ
к приказу директора РГП «ГРС»
от «___» _____2020 года
№_____

№	Наименование документа
1.	Политика информационной безопасности
2.	Методика оценки рисков информационной безопасности
3.	Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации
4.	Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации
5.	Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения
6.	Правила проведения внутреннего аудита ИБ
7.	Правила использования средств криптографической защиты информации
8.	Правила разграничения прав доступа к электронным информационным ресурсам
9.	Правила использования Интернет и электронной почты
10.	Правила организации процедуры аутентификации
11.	Правила организации антивирусного контроля
12.	Правила использования мобильных устройств и носителей информации
13.	Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов
14.	Каталог угроз (рисков) ИБ
15.	План обработки угроз (рисков) ИБ
16.	Регламент резервного копирования и восстановления информации
17.	План мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации
18.	Руководство администратора по сопровождению объекта информатизации
19.	Инструкцию о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях
20.	Журналы

Утверждаю
Директор
РГП «Государственная
радиочастотная служба»
_____Р.Нуршабеков
«_____» _____2020 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нур-султан– 2020 год

СОДЕРЖАНИЕ

1. СОКРАЩЕНИЯ

1. **АХО** – Административно-хозяйственный отдел.
2. **ДРИ** – Департамент развития инфраструктуры.
3. **ИБ** – Информационная безопасность.
4. **ИС** – Информационная система.
5. **ОБУ** – Отдел бухгалтерского учета.
6. **ПО** – Программное обеспечение.
7. **РГП «ГРС»** – Республиканское государственное предприятие «Государственная радиочастотная служба».
8. **РК** – Республика Казахстан.
9. **СИБ** – Сектор информационной безопасности.
10. **СУБД** – Система управления базами данных.

2. ОПРЕДЕЛЕНИЯ

1. **Информационная безопасность** (далее – ИБ) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;
2. **Информационная система** (далее – ИС) – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;
3. **Инцидент информационной безопасности** – отдельно или серийно возникающий сбой в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающий угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;
4. **Конфиденциальная информация** – все виды информации (включая коммерческую, банковскую, налоговую, личную, адвокатскую тайну), в отношении которой в соответствии с нормативными правовыми актами ограничен доступ (установлена конфиденциальность);
5. **Локальная сеть** – часть сети телекоммуникаций, имеющая замкнутую инфраструктуру до точки подключения к другим сетям телекоммуникаций и обеспечивающая передачу информации и организацию совместного доступа к сетевым устройствам в территориально ограниченном пространстве объекта (помещение, здание, сооружение и его комплекс);
6. **Электронные информационные ресурсы** – информация, предоставленная в электронно-цифровой форме и содержащаяся на электронном носителе, интернет-ресурсе и (или) в информационной системе.

3. ОБЛАСТЬ ПРИМЕНЕНИЯ

1. Настоящая Политика распространяется на информационные системы РГП «ГРС» и является обязательной для исполнения всеми пользователями, работающими в них.

4. ОПИСАНИЕ
4.1 ОБЩЕЕ ПОЛОЖЕНИЕ

2. Настоящая Политика информационной безопасности (далее – Политика) предназначена для определения целей и требований обеспечения информационной безопасности информационных систем Республиканское государственное предприятие «Государственная радиочастотная служба» (далее – РГП «ГРС»).
3. Настоящая Политика учитывает современное состояние и ближайшие перспективы развития информационно-коммуникационной инфраструктуры РГП «ГРС», цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее ресурсов.
4. Политика является методологической базой для:
1) выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;
2) обеспечения информационной безопасности;
3) координации деятельности структурных подразделений РГП «ГРС» при проведении работ по соблюдению требований по обеспечению информационной безопасности.
5. Научно-методической основой настоящей Политики является системный подход, предполагающий проведение исследований, разработку системы защиты информации в процессе ее обработки в информационной системе с учетом всех факторов, оказывающих на нее влияние и комплексного применения различных мер и средств защиты.
6. Основные положения настоящей Политики базируются на качественном осмыслении вопросов информационной безопасности, не концентрируя внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

4.2 ЦЕЛИ ПОЛИТИКИ

7. Основными целями Настоящей Политики являются:
1) обеспечение доступности обрабатываемой информации для зарегистрированных пользователей;
2) устойчивое функционирование информационно-коммуникационной инфраструктуры РГП «ГРС»;

3) обеспечение конфиденциальности информации, обрабатываемой средствами вычислительной техники и передаваемой по каналам связи;
4) обеспечение целостности и аутентичности информации, хранящейся и обрабатываемой в информационной системе РГП «ГРС» и передаваемой по каналам связи.

4.3 ЗАДАЧИ ПОЛИТИКИ

8. Для достижения целей поставлены следующие задачи:
1) формирование и проведение единой политики в области обеспечения информационной безопасности в РГП «ГРС»;
2) обеспечение непрерывности деятельности информационных систем, организационно-методических и технических мероприятий, направленных на минимизацию последствий утраты информационных активов посредством комплекса предупреждающих и восстанавливающих мероприятий;
3) определение процедур, направленных на выявление, отражение и последующую ликвидацию последствий различных видов угроз безопасности;
4) управление рисками в целях недопущения или снижения вероятности возникновения внештатных ситуаций;
5) определение требований к содержанию процедур по управлению информатизацией в рамках РГП «ГРС» с учетом обеспечения информационной безопасности;
6) разработка предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения информационной безопасности РГП «ГРС»;
7) определение нормативных правовых, технологических и организационных процедур.

4.4 ОСНОВНЫЕ ПРИНЦИПЫ НАСТОЯЩЕЙ ПОЛИТИКИ

9. Настоящая Политика основывается на принципах:
1) обеспечения информационной безопасности путем сохранения конфиденциальности, целостности и доступности информации;
2) конфиденциальности путем предоставления доступа к информации только авторизованным лицам;
3) целостности путем внесения исключительно авторизованных изменений в ИС, общедоступные электронные информационные ресурсы (данные находящиеся на персональных компьютерах, в корпоративной электронной почте, система электронного документооборота и т.д.);
4) доступности путем предоставления авторизованным лицам доступа в ИС, общедоступные электронные информационные ресурсы (данные находящиеся на персональных компьютерах, в корпоративной электронной почте и т.д.) для выполнения их служебных обязанностей.

4.5 ОРГАНИЗАЦИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10. В целях разграничения ответственности и функций в сфере обеспечения информационной безопасности, структурное подразделение ИБ должно быть обособлено от подразделений, занимающихся вопросами создания, сопровождения и развития объектов информатизации.
11. В организации обеспечения информационной безопасности РГП «ГРС» участвуют:
1) Сектор информационной безопасности РГП «ГРС» (далее – СИБ) – ответственное подразделение за обеспечение информационной безопасности в РГП «ГРС»;
2) Департамент развития инфраструктуры (далее – ДРИ) – ответственное подразделение за информатизацию, администрирование, сопровождение и обеспечение бесперебойного функционирования всего аппаратно-программного комплекса РГП «ГРС»;
3) Администратор информационных систем (далее – администратор) – специалист, ответственный за администрирование, сопровождение и обеспечение бесперебойного функционирования всего аппаратно-программного комплекса;

К администраторам информационных систем РГП «ГРС» относятся работники ДРИ, на которых директором ДРИ возложены функции в рамках служебных обязанностей по администрированию прикладного программного обеспечения (далее – ППО), систем управления базами данных (далее – СУБД), операционных систем (далее – ОС) и т.д.;
4) Отдел бухгалтерского учета РГП «ГРС» (далее – ОБУ) и Административно-хозяйственный отдел РГП «ГРС» (далее – АХО)– ответственное подразделение за инвентаризацию активов РГП «ГРС»;
5) АХО – ответственное подразделение за бесперебойную работу коммунальных систем РГП «ГРС»;
12. СИБ организует, выполняет, контролирует и координирует вопросы и работы, связанные с защитой информации и осуществляет:
1) контроль за исполнением требований настоящей Политики;
2) контроль за документальным оформлением информационной безопасности (заполнение журналов, включенных в документы 4 уровня Политики);
3) контроль за управлением активами в части обеспечения информационной безопасности;
4) контроль законности использования программного обеспечения;
5) контроль за управлением рисками;
6) контроль за регистрацией событий информационной безопасности;
7) проведение планового и внепланового аудита информационной безопасности;

8) проведение внутреннего и внешнего аудита информационной безопасности;
9) управление непрерывностью бизнес-процессов и контроль за его осуществлением;
10) контроль соблюдения требований информационной безопасности при управлении персоналом;
11) контроль и внедрение функционирования системы обеспечения информационной безопасности;
12) разъяснение норм настоящей Политики для работников РГП «ГРС».
13. Для достижения целей настоящей Политики руководство РГП «ГРС» обеспечивает:
1) ведение контроля за эффективностью реализации настоящей Политики;
2) распределение функциональных ролей и обязанностей по информационной безопасности.
14. СИБ вносит предложения руководству РГП «ГРС» по основным направлениям развития мер, направленных на защиту информации от несанкционированного доступа и инициирование планов и программ по поддержанию осведомлённости об информационной безопасности.
15. Для достижения поставленных задач в области информационной безопасности СИБ:
1) мониторит и контролирует информационно-коммуникационную инфраструктуру РГП «ГРС»;
2) имеет доступ во все помещения РГП «ГРС», где установлены: средства вычислительной техники, локальная сеть и средства обработки информации;
3) осуществляет прекращение автоматизированной обработки информации при наличии непосредственной угрозы для защищаемой информации.

5. ПЕРЕСМОТР ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

16. Развитие, пересмотр и оценку информационной безопасности осуществляет СИБ.
17. Пересмотр настоящей Политики производится в целях:
1) усовершенствования целей и мер контроля информационной безопасности;
2) усовершенствования подхода к управлению информационной безопасности и бизнес-процессами РГП «ГРС»;
3) улучшения распределения ресурсов и/или обязанностей.
18. При появлении существенных изменений в технологиях, обеспечивающих информационную безопасность, в целях обеспечения конфиденциальности, целостности, доступности информации, а также эффективности применяемых мер.

19. Допускается руководством РГП «ГРС» инициирование внепланового пересмотра настоящей Политики. Такой пересмотр проводится лицом, не имеющим прямого отношения к пересматриваемой области безопасности. Результаты независимого пересмотра документируются и оформляются в виде отчета и доводятся до руководства.
20. Настоящая Политика пересматривается в случае изменения общих политик безопасности информации и ее ценностей, а также после проведения анализа и оценки рисков информационной безопасности для РГП «ГРС», по итогам которых, с учетом исправления выявленных недостатков требуется ее актуализация.
21. При каждом пересмотре настоящей Политики учитываются инциденты, послужившие причиной для предыдущих пересмотров.

6. КОНТРОЛЬ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

22. Контроль требований настоящей Политики информационной безопасности на соответствие требованиям информационной безопасности осуществляет СИБ.

7. БАЗОВАЯ ССЫЛКА

Настоящая Политика разработана в соответствии со следующими нормативными правовыми актами:

1) Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации»;
2) Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;
3) Государственный стандарт Республики Казахстан СТ РК 34.005-2002 «Информационная технология. Основные термины и определения»;
4) Государственный стандарт Республики Казахстан СТ РК 34.006-2002 «Информационная технология. Базы данных. Основные термины и определения»;
5) Государственный стандарт Республики Казахстан СТ РК 34.007-2002 «Информационная технология. Телекоммуникационные сети. Основные термины и определения»;
6) Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защиты информации».
7) Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования».

8. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

№	№ раздела, подраздела, пункта стандарта, к которому относится изменение	Номер листа	Дата введения изменения	Основание (№ и дата приказа)	Дата внесения изменения	Подпись лица, внесшего изменения

9. ЛИСТ ОЗНАКОМЛЕНИЯ

№	Ф.И.О.	Занимаемая должность	Дата	Подпись	Примечание