	Политика информационной безопасности	ДО-12-2025

УТВЕРЖДАЮ
Генеральный директор
ФГБУ «Авиаметтелеком Росгидромета»
_____ В.С. Пьянков
«15» 09 2025 г.

Политика информационной безопасности ФГБУ «Авиаметтелеком Росгидромета»

Введена в действие с 17.09 2025 приказом от 15.09.2025 № 320	Введена впервые	г. Москва 2025

ВНЕСЕНО:

Заместитель генерального директора
ФГБУ «Авиаметтелеком Росгидромета»
_____ Г.Г. Варелджян
«25» августа 2025 г.

СОГЛАСОВАНО:

Заместитель генерального директора
ФГБУ «Авиаметтелеком Росгидромета»
_____ В.В. Цуканов
«15» сентября 2025 г.

Заместитель генерального директора
ФГБУ «Авиаметтелеком Росгидромета»
_____ С.В. Коршунов
«25» августа 2025 г.

Заместитель генерального директора
ФГБУ «Авиаметтелеком Росгидромета»
_____ Э.В. Тупичкин
«04» сентября 2025 г.

Заместитель генерального директора
ФГБУ «Авиаметтелеком Росгидромета»
_____ Р.Р. Хамитов
«27» 08 2025 г.

Главный бухгалтер
ФГБУ «Авиаметтелеком Росгидромета»
_____ Е.Л. Григорьевская
«15» сентября 2025 г.

Заместитель начальника юридического отдела ФГБУ «Авиаметтелеком Росгидромета»
_____ Д.Л. Степин
«28» августа 2025 г.

Представитель руководства по качеству
ФГБУ «Авиаметтелеком Росгидромета»
_____ В.Д. Тедикова
«27» 08 2025 г.

Содержание

1	Введение	5
2	Термины, определения и сокращения	7
3	Цели и задачи информационной безопасности	8
4	Объекты обеспечения информационной безопасности	9
5	Основные угрозы информационной безопасности	9
6	Принципы обеспечения информационной безопасности	10
7	Управление рисками информационной безопасности	14
8	Основные направления информационной безопасности	15
8.1	Документирование требований по ИБ	15
8.2	Организация ИБ	15
8.3	Аудит и контроль соблюдения требований ИБ	16
8.4	Управление информационными активами	16
8.5	Управление доступом к информационным активам	17
8.6	Защита от вредоносного кода	17
8.7	Защита от утечек информации	17
8.8	Управление носителями информации	18

8.9	Безопасность сетевой инфраструктуры	18
8.10	Мониторинг и регистрация событий	18
8.11	Управление уязвимостями	18
8.12	Управление инцидентами ИБ	19
8.13	Обеспечение безопасности на этапах жизненного цикла ИС	19
8.14	Использование АРМ и ИС	20
8.15	Использование ПО	20
8.16	Управление изменениями	20
8.17	Использование информационных ресурсов	21
8.18	Резервное копирование и восстановление информации	21
8.19	Управление непрерывностью деятельности	21
8.20	Обеспечение безопасности при работе с персоналом	22
8.21	Повышение осведомленности в области ИБ	22
8.22	Обеспечение безопасности при взаимодействии с третьими лицами	22
8.23	Организация физической защиты	23
8.24	Применение технических средств защиты информации	23
9	Ответственность	24
10	Лист регистрации изменений	27
11	Лист регистрации ознакомлений	28

1 Введение

1.1 Политика информационной безопасности (далее – Политика) Федерального государственного бюджетного учреждения «Главный центр информационных технологий и метеорологического обслуживания авиации» (далее – ФГБУ «Авиаметтелеком Росгидромета», Учреждение) является основополагающим документом, который регламентирует процессы обеспечения информационной безопасности в Учреждении, включая филиалы. Политика содержит комплекс принципов, правил, процедур и руководящих инструкций для защиты информационных активов Учреждения от рисков, возникающих в результате реализации угроз информационной безопасности.

1.2 Политика представляет собой систематизированное изложение высокоуровневых целей и задач по обеспечению информационной безопасности (далее – ИБ), которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы управления информационной безопасностью (далее – СУИБ) Учреждения.

1.3 Настоящая Политика выражает позицию Учреждения в области информационной безопасности. Принятием настоящей Политики Учреждение провозглашает и обязуется осуществлять все возможные меры для защиты работников, имущества, информации, деловой репутации и бизнес-процессов Учреждения, включая филиалы, от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз ИБ.

1.4 Настоящая Политика распространяется на все структурные подразделения Учреждения, включая филиалы, и обязательна для исполнения всеми работниками и должностными лицами.

1.5 Настоящая Политика не распространяется на организацию и порядок защиты информации, составляющей государственную тайну.

1.6 Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

1.7 Лица, осуществляющие разработку внутренних документов Учреждения, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

1.7.1 Настоящая Политика является локальным нормативным документом постоянного действия.

1.8 Настоящая Политика, а также все изменения к ней утверждаются генеральным директором Учреждения и вводятся в действие приказом Учреждения.

1.9 Настоящая Политика подлежит регулярному пересмотру не реже 1 раза в год, а также в следующих случаях:

– изменения требований законодательства Российской Федерации, нормативных документов регуляторов в области ИБ;

– существенных изменений в информационной инфраструктуре или организационной структуре Учреждения;

– выявления инцидентов ИБ, свидетельствующих о неполноте или несовершенстве настоящей Политики.

1.10 Предпосылками для пересмотра и совершенствования настоящей Политики могут также являться результаты мониторинга состояния ИБ, результаты анализа актуальных внутренних и внешних угроз, а также результаты анализа нарушений, выявленных в ходе внутреннего и внешнего контроля (несоответствие реальных технологий и состояния информационной безопасности требованиям нормативных и регламентирующих документов).

2 Термины, определения и сокращения

2.1 В Политике используются следующие термины и определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.

Информационный актив – все, что имеет ценность для ФГБУ «Авиаметтелеком Росгидромета» в информационной сфере (информация, программное обеспечение, технические средства обработки информации, средства связи, работники и прочее).

2.2 В Политике используются следующие сокращения:

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
ОТП	Отдел технической поддержки
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ФГБУ	Федеральное государственное бюджетное учреждение
СКУД	Система контроля и управления доступом
СУИБ	Система управления информационной безопасностью
СЭДО	Система электронного документооборота
ЭП	Электронная подпись

3 Цели и задачи информационной безопасности

3.1 Основной целью Учреждения в области обеспечения ИБ является минимизация рисков ИБ, которым подвержены технологии и информационные системы, используемые для достижения целей Учреждения, а также обеспечение эффективности мероприятий по ликвидации неблагоприятных последствий реализации угроз и инцидентов ИБ.

3.2 Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации – устойчивого функционирования ИС Учреждения, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время;
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в ИС Учреждения и передаваемой по каналам связи;
- конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.

3.3 Достижение основной цели должно обеспечиваться решением следующих задач:

- вовлечение руководителей прямого подчинения генеральному директору Учреждения, в том числе директоров филиалов, в процесс обеспечения ИБ;
- документирование требований ИБ;
- реализация мер по защите информационных ресурсов Учреждения от угроз ИБ;
- оптимизация стоимости владения средствами защиты информации в рамках Учреждения;
- прогнозирование угроз и оценка рисков ИБ;
- предотвращение и/или снижение до приемлемого уровня ущерба от реализации актуальных угроз ИБ в Учреждении;
- соблюдение законодательных и нормативных требований в области ИБ, включая требования регуляторов в области ИБ;
- обеспечение стабильности функционирования Учреждения в условиях возможной реализации угроз ИБ;
- оперативное реагирование на инциденты ИБ;
- контроль состояния ИБ Учреждения;
- повышение осведомленности работников Учреждения в вопросах обеспечения ИБ;
- постоянное совершенствование систем обеспечения ИБ Учреждения, включая проводимую политику обеспечения и управления ИБ.

3.4 Обеспечение ИБ включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Учреждение.

4 Объекты обеспечения информационной безопасности

4.1 В рамках обеспечения ИБ объектами защиты в Учреждении являются: информация, обрабатываемая в Учреждении, вне зависимости от формы представления; информационные ресурсы, включая, но не ограничиваясь следующим перечнем:

- автоматизированные рабочие места, средства обработки информации и мобильные технические средства;
- информационные системы, системы хранения данных, программное обеспечение и отдельные технические решения;
- автоматизированные системы управления, системы передачи данных, измерительные системы и системы автоматизации технологических (производственных) процессов;
- ИТ-инфраструктура, информационно-телекоммуникационные сети и системы связи;
- ИТ-сервисы (ИТ-услуги), оказываемые Учреждением или в интересах Учреждения.

4.2 Перечень объектов обеспечения ИБ, определяется по результатам инвентаризации (учета) и классификации, проводимой в соответствии с установленным в Учреждении порядком, описанным отдельным внутренним документом.

5 Основные угрозы информационной безопасности

5.1 Основные угрозы ИБ включают в себя:

- несанкционированный доступ к защищаемой информации Учреждения;
- компрометацию паролей, персональных идентификаторов и другой ключевой информации;
- вирусное заражение;
- уничтожение (утеря) защищаемой информации;
- разглашение защищаемой информации;
- злонамеренные действия, осуществляемые посредством локальной вычислительной сети Учреждения;
- целенаправленные атаки на информационные системы Учреждения с использованием уязвимостей «нулевого дня»;
- нештатная ситуация в работе программного обеспечения информационных систем Учреждения;
- выход из строя материальных носителей защищаемой информации;

- выход из строя программно-технических средств Учреждения;
- нарушение функционирования технических мер защиты;
- ввод некорректных (ложных) данных в информационные системы Учреждения;
- несанкционированное или некорректное внесение изменений в информационные системы Учреждения;
- несанкционированное делегирование полномочий и/или использование привилегий;
- халатность, игнорирование установленных правил обеспечения ИБ, увеличивающие вероятность реализации угрозы ИБ;
- угрозы нарушения целостности и функционирования Учреждения в целом.

5.2 Источники угроз ИБ делятся на два основных класса:

- источники, связанные с действиями людей – внешние и внутренние нарушители;
- источники, связанные с природными явлениями (стихийными бедствиями) и неблагоприятными техногенными факторами.

5.3 В качестве внешних нарушителей ИБ рассматриваются лица, не входящие в состав пользователей и обслуживающего персонала ИС Учреждения, например, разработчики ИС, внешние лица (хакеры, члены криминальных организаций, бывшие работники Учреждения и т.п.).

5.4 В качестве потенциальных внутренних нарушителей ИБ рассматриваются пользователи и обслуживающий персонал ИС Учреждения, другие субъекты (лица), вовлеченные в информационные процессы Учреждения, которые также имеют возможность санкционированного доступа к ИС Учреждения.

5.5 Перечень угроз ИБ и нарушителей безопасности определяется в ходе процедуры моделирования угроз (Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021)) и закрепляется в Модели угроз Учреждения.

6 Принципы обеспечения информационной безопасности

6.1 В основе реализации обеспечения ИБ лежит комплексный подход, который включает в себя следующие группы мер защиты информации:

- нормативно-правовые;
- организационные;
- программно-технические.

6.2 Реализация Политики должна осуществляться из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные

разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий.

6.3 При построении ИБ Учреждение руководствуется следующими основополагающими принципами:

6.3.1 **Неотъемлемость.** Безопасность информационной системы является ее неотъемлемым свойством (характеристикой), а не дополнительным сервисом. Соблюдение требований ИБ должно быть обязательным для всех работников и являться частью корпоративной культуры Учреждения.

6.3.2 **Комплексность.** Необходимо согласованное применение разнородных средств при построении целостной системы защиты информации, перекрывающей все каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами, обеспечивающими в комплексе инженерно-техническую защиту объектов, защиту от несанкционированного доступа к компьютерам пользователей и серверам, разграничение доступа работников к информационным ресурсам, защиту каналов обмена информацией, защиту информации от утечек по техническим каналам и т.д.

6.3.3 **Системность.** Деятельность по защите информации должна быть строго и всесторонне регламентирована – Политика как совокупность норм, требований, положений, порядков и инструкций, должна учитывать все наиболее слабые и уязвимые места ИС и охватывать весь их жизненный цикл. При этом необходим учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения ИБ в ИС. Необходим анализ и учет всех текущих слабых и уязвимых мест ИС, возможных объектов и направлений атак, и, учитывая высокую квалификацию злоумышленников, возможных в будущем каналов реализации угроз ИБ.

6.3.4 **Непрерывность.** Обеспечение ИБ – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС Учреждения, начиная с самых ранних стадий их проектирования.

6.3.5 **Адекватность.** Применяемые методы и средства защиты информации должны быть адекватны угрозам ее уничтожения, утечке или искажения. Недопустима как недостаточная, так и чрезмерная защита. Создать абсолютно защищенную систему принципиально невозможно, взлом системы есть вопрос только времени и средств. В связи с этим, при проектировании систем защиты информации необходимо говорить только о некотором приемлемом уровне безопасности. Важно выбрать золотую середину между стойкостью защиты и ее стоимостью, потреблением вычислительных ресурсов, удобством работы пользователей и другими характеристиками систем защиты

информации. Информационная система – результат компромисса между функциональностью и безопасностью.

6.3.6 **Идентификация и оценка.** Реализация этого принципа должна основываться на идентификации всех информационных систем и определении их ценности для целей и задач Учреждения.

6.3.7 **Гибкость и управляемость.** Системы защиты информации должны обеспечивать возможность изменять уровень защищенности ИС. Гибкость управления и применения системы защиты информации избавляет от необходимости принятия кардинальных мер по полной замене средств защиты на новые при смене условий функционирования защищаемых систем. В целях обеспечения гибкости и управляемости защиты ИС, при выборе между организационными и техническими мерами, приоритет должен отдаваться мерам технического характера.

6.3.8 **Своевременность.** Разработка системы обеспечения ИБ должна вестись вместе с разработкой защищаемой системы. Недопустима ситуация, когда та или иная система разработана и вводится в эксплуатацию, а затем делаются попытки ее защитить. Разработка системы обеспечения ИБ, осуществляемая параллельно разработке защищаемой системы, оптимизирует затраты ресурсов и позволяет вырабатывать наиболее эффективные решения.

6.3.9 **Упреждение.** Акцент в работе системы обеспечения ИБ должен делаться на предотвращении (предупредительных мерах) событий ИБ, которые могут повлиять на целостность, доступность и конфиденциальность информации.

6.3.10 **Контролируемость.** Постоянный контроль ИБ Учреждения, выявление и устранение уязвимостей, мониторинг событий, влияющих на ее состояние, является обязательной составляющей эффективной системы обеспечения ИБ.

6.3.11 **Анализ и совершенствование.** Необходима постоянная работа по улучшению существующей практики и совершенствованию средств и методов управления и обеспечения информационной безопасности на основе результатов аудитов информационной безопасности, мониторинга функционирования систем информационной безопасности, анализа изменений в методах и средствах компьютерных атак, анализа нормативных требований и существующего передового отечественного и зарубежного опыта в этой области.

6.3.12 **Минимизация полномочий.** Предоставление пользователям прав доступа определяется исключительно производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, в каком это минимально необходимо работнику для выполнения его должностных обязанностей.

6.3.13 **Разделение функций.** При определении состава ролей, использующихся для распределения прав доступа, запрещается совмещение в рамках одной роли такого

состава функций (концентрации полномочий), которое позволило бы одному работнику единолично осуществлять выполнение критичных операций или получать полный и неконтролируемый доступ к какой-либо системе Учреждения. Исключение единоличного совершения критичной операции может быть организовано на уровне организационных мер и/или программно-технических средств за счет выделения полномочий или роли пользователя. Программно-технический способ разделений полномочий является предпочтительным относительно организационного. Действия работников, обладающих административными полномочиями, должны находиться под особым контролем со стороны структурного подразделения по обеспечению ИБ.

6.3.14 **Персонификация.** Действия всех работников Учреждения должны осуществляться от имени персонифицированной учетной записи. Такая учетная запись у каждого работника должна быть единственной в связи с тем, что наличие у работника двух и более учетных записей делает не эффективной систему распределения и контроля полномочий. Исключение по решению руководства Учреждения могут составлять администраторы систем, должностные обязанности которых предполагают внесение изменений в указанные системы. Для них в дополнение к учетной записи с стандартными правами пользователя, может быть создана административная учетная запись с расширенными привилегиями. Наличие учетных записей, не закрепленных за конкретным работником, не допустимо.

6.3.15 **Запрещено все, что не разрешено.** Доступ к любой ИС должен предоставляться только при наличии соответствующего разрешения (правила), зафиксированного в документации к ИС, регламенте бизнес-процесса и настройках средств защиты информации. Любой доступ (не разрешенный явно) должен быть запрещен. Функция безопасности – разрешать необходимые доступы. Такой подход обеспечивает только известные безопасные доступы (действия) и освобождает от необходимости распознавать любую угрозу.

6.3.16 **Простота применения защитных мер и средств.** Используемые средства зашиты информации должны быть интуитивно понятны и просты в использовании. Их применение не должно быть связано со значительными дополнительными трудозатратами при обычной работе пользователей ИС.

6.3.17 **Эшелонированность средств защиты.** Нельзя полагаться на единственный защитный рубеж, каким бы надежным он не считался. Помимо средств защиты периметра должны использоваться системы защиты внутренней сети, серверов, рабочих станций, баз данных и т.д.

6.3.18 **Осведомленность** работников Учреждения в вопросах ИБ – обязательное условие безопасного функционирования систем. Необходимо не только информировать всех работников Учреждения и третьих лиц, использующих ИС Учреждения, о требованиях информационной безопасности, но развивать навыки приемлемого

обращения с информацией и безопасной работы с ИС Учреждения.

6.3.19 **Персональная ответственность.** Ответственность за обеспечение безопасности информации и систем ее обработки возлагается не только на структурное подразделение по обеспечению ИБ, но и на каждого работника организации в пределах его полномочий. Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с настоящей Политикой, должны быть доведены до работника при трудоустройстве и внесены в его должностные обязанности. Все принимаемые на работу работники должны одобрить и подписать свои трудовые договоры, в которых устанавливается их ответственность за ИБ. В трудовой договор должно быть включено согласие работника на проведение контрольных мероприятий со стороны Учреждения по проверке выполнения требований ИБ, а также обязательства по неразглашению конфиденциальной информации. В трудовом договоре должны быть описаны меры, которые будут приняты в случае несоблюдения работником требований ИБ.

6.3.20 **Лояльность персонала.** Необходимо создание благоприятной атмосферы во всех структурных подразделениях Учреждения, при которой выполнение требований ИБ не воспринимается работниками как дополнительная нагрузка, от которой желательно избавиться, а воспринимается как осознанная необходимость и неотъемлемая часть корпоративной этики. В указанной обстановке работники осознанно соблюдают установленные правила и требования ИБ и эффективно взаимодействуют со структурным подразделением по обеспечению ИБ.

6.3.21 **Вовлеченность руководства.** Необходимо осознание руководством Учреждения необходимости обеспечения ИБ, непосредственного участия в принятии стратегических решений по вопросам функционирования системы обеспечения ИБ, включая вопросы принятия рисков.

6.3.22 **Взаимодействие и координация.** Эффективное обеспечение ИБ достигается на основе взаимодействия и координации со всеми заинтересованными структурными подразделениями Учреждения.

7 Управление рисками информационной безопасности

7.1 Обеспечение ИБ Учреждения основывается на управлении рисками ИБ, что предусматривает анализ существующих угроз ИБ, оценку рисков реализации указанных угроз и принятие необходимых мер (в том числе применение средств защиты информации) по отношению к рискам ИБ, недопустимым для Учреждения.

7.2 Целью управления рисками ИБ является:

- минимизация негативных последствий от реализации рисков;
- оптимизация затрат, направленных на предотвращение негативных последствий от реализации рисков.

7.3 Порядок управления рисками должен регламентироваться отдельным внутренним документом Учреждения.

7.4 Ответственным за процесс управления рисками ИБ в Учреждении является структурное подразделение отвечающее за ИБ Учреждения.

8 Основные направления информационной безопасности

8.1 Документирование требований по ИБ

8.1.1 В Учреждении должен быть разработан, утвержден и доведен до работников комплект документов (политик, положений, инструкций), регламентирующих отдельные направления ИБ.

8.1.2 Документы по ИБ для гарантии их постоянной актуальности, соответствия и результативности должны пересматриваться через запланированные интервалы времени, а также в случаях:

- изменений требований законодательства Российской Федерации, нормативных документов регуляторов в области ИБ;
- существенных изменений бизнес-процессов Учреждения, информационной инфраструктуры, организационной структуры Учреждения;
- выявления инцидентов ИБ, свидетельствующих о неполноте или несовершенстве имеющихся документов по ИБ.

8.1.3 Предпосылками для пересмотра и совершенствования документов по ИБ могут также являться результаты мониторинга состояния ИБ, результаты анализа актуальных внутренних и внешних угроз, а также результаты анализа нарушений, выявленных в ходе внутреннего и внешнего контроля (несоответствие реальных технологий и состояния информационной безопасности требованиям нормативных и регламентирующих документов).

8.1.4 Руководители структурных подразделений Учреждения в пределах своей области ответственности должны регулярно анализировать соответствие обработки информации и процедур требованиям внутренних документов Учреждения по ИБ, в том числе требованиям настоящей Политики.

8.2 Организация ИБ

8.2.1 Управление ИБ должно обеспечиваться как при осуществлении информационного обмена внутри Учреждения, так и при взаимодействии со сторонними организациями и третьими лицами (субъектами).

8.2.2 В Учреждении, включая филиалы, должны быть назначены структурное подразделение и/или лица, ответственные за обеспечение ИБ, в том числе за организацию планирования, совершенствования и развития обеспечения и управления ИБ. Ответственные за обеспечение ИБ должны быть назначены приказом, а обязанности

ответственных лиц должны быть определены в их должностных инструкциях.

8.2.3 Для снижения возможностей несанкционированного ознакомления, удаления, модификации, искажения и (или) злоупотребления информационными активами в Учреждении должен соблюдаться принцип разделения сфер ответственности. Этот принцип должен учитываться при организации всех мероприятий по ИБ в Учреждении, в том числе при обеспечении доступа к информационным активам Учреждения тех работников Учреждения и третьих лиц, которым это объективно необходимо, исходя из степени их ответственности, функциональных обязанностей, решаемых задач и условий заключенных договоров.

8.2.4 При выборе средств обеспечения и контроля ИБ Учреждение должно ориентироваться на использование отечественных продуктов, в том числе на использование отечественного системного и прикладного ПО, вычислительной техники и сетевого оборудования.

8.3 Аудит и контроль соблюдения требований ИБ

8.3.1 Для оценки эффективности применяемых мер и средств обеспечения ИБ, а также пригодности и адекватности подхода к обеспечению ИБ, в Учреждении должны периодически проводиться мероприятия по аудиту (проверке) ИБ.

8.3.2 Аудит ИБ может быть как внутренним, так и внешним. Цель, порядок и периодичность проведения аудитов ИБ структурных подразделений Учреждения должны указываться в программе аудита ИБ. Порядок проведения внутреннего аудита ИБ определяется отдельным внутренним документом Учреждения.

8.3.3 При проведении аудитов ИБ должны использоваться стандартные процедуры документальной проверки, опрос и интервью с руководством и персоналом организации и технические процедуры тестирования (тестирование на проникновение, нагрузочное стресс тестирование).

8.3.4 К проведению внутренних аудитов ИБ могут привлекаться специалисты, обладающие специальными навыками и знаниями, имеющими значение для проведения аудита.

8.4 Управление информационными активами

8.4.1 Защите подлежит любая информация, принадлежащая Учреждению или переданная Учреждению контрагентом в рамках договорных отношений. Все информационные активы Учреждения должны защищаться в соответствии с их степенью важности для достижения целей Учреждения.

8.4.2 Порядок классификации и управления информационными активами должен регламентироваться отдельным внутренним документом Учреждения.

8.5 Управление доступом к информационным активам

8.5.1 Управление доступом (в т.ч. удаленного) к информационным активам Учреждения должно определяться принципами предоставления работникам и иным третьим лицам минимально необходимых для осуществления их деятельности привилегий. Доступ к информационным активам Учреждения должен предоставляться по согласованию с ответственным (владельцем) за информационный актив и структурным подразделением (лицом) ответственным за информационную безопасность только на основании документально обоснованной производственной необходимости (распоряжение (приказ), подписанная служебная записка, электронное письмо и т.д.).

8.5.2 Подходы к управлению доступом (в т.ч. удаленным доступом) должны регламентироваться отдельным внутренним документом Учреждения.

8.6 Защита от вредоносного кода

8.6.1 В Учреждении должны быть реализованы меры защиты от вредоносного программного обеспечения (вредоносного кода) для всех компонентов информационной инфраструктуры.

8.6.2 Должны быть внедрены меры обнаружения, предупреждения и восстановления последствий воздействия вредоносного кода.

8.6.3 Вопросы защиты от вредоносного кода должны регламентироваться отдельным внутренним документом Учреждения.

8.7 Защита от утечек информации

8.7.1 В Учреждении должны осуществляться мероприятия для защиты информации от ее несанкционированного разглашения (утечки). В рамках данных мероприятий должен осуществляться контроль следующей информации:

- информации, передаваемой в информационно-телекоммуникационную сеть «Интернет»;
- информации, передаваемой с использованием средств электронной почты;
- информации, передаваемой на печать;
- информации, записываемой на съемные носители.

8.7.2 Распространение информации и передача информационных активов (за исключением общедоступной информации) должны быть запрещены, если только такое действие не осуществляется согласно случаям, предусмотренным законодательством Российской Федерации, внутренними документами Учреждения, включая Политику.

8.7.3 При переводе работника Учреждения на другое место работы, вынос информационных активов из структурного подразделения, в котором он работал до перевода, запрещен, за исключением случаев, когда такие действия осуществляются в соответствии с внутренними документами Учреждения, включая Политику.

8.7.4 Работники Учреждения не должны распространять информацию об Учреждении. Это касается всех работников Учреждения, вне зависимости от их положения, должности или деятельности в нерабочее время.

8.7.5 Дополнительные требования в части защиты от утечек информации должны регламентироваться отдельным внутренним документом Учреждения.

8.8 Управление носителями информации

8.8.1 В Учреждении должен вестись учет всех носителей защищаемой информации, как в письменном, так и в электронном виде. В рамках данного учета должен вестись реестр носителей информации.

8.8.2 Все носители информации должны быть снабжены признаками, позволяющими идентифицировать носитель информации и хранящуюся на нем информацию.

8.8.3 Порядок работы с носителями информации должен регламентироваться отдельным внутренним документом Учреждения.

8.9 Безопасность сетевой инфраструктуры

8.9.1 В Учреждении должно быть обеспечено управление безопасностью телекоммуникационных сетей и ее элементов, ответственность за эксплуатацию которых несет Учреждение, включая постоянный мониторинг состояния сетевой безопасности сети.

8.9.2 Вопросы обеспечения безопасности сетевой инфраструктуры должны регламентироваться отдельным внутренним документом Учреждения.

8.10 Мониторинг и регистрация событий

8.10.1 В Учреждении должны осуществляться регулярный мониторинг и регистрация системных событий, действий пользователей и администраторов, ошибок и событий ИБ.

8.10.2 Все зарегистрированные события должны анализироваться на предмет наличия признаков инцидента ИБ.

8.10.3 Вопросы регистрации и мониторинга событий должны регламентироваться отдельным внутренним документом Учреждения.

8.11 Управление уязвимостями

8.11.1 В Учреждении должен быть организован процесс управления уязвимостями, включающий в себя постоянное выявление, анализ и устранение

выявленных уязвимостей.

8.11.2 Должны проводиться регулярные работы по тестированию на проникновение, как во внешние, так и во внутренние сети Учреждения.

8.11.3 Вопросы управления уязвимостями должны регламентироваться отдельным внутренним документом Учреждения.

8.12 Управление инцидентами ИБ

8.12.1 В Учреждении должен быть организован процесс управления инцидентами ИБ, в рамках которого каждый инцидент ИБ должен фиксироваться и расследоваться. Результаты служебного расследования должны доводиться до руководства Учреждения. По каждому случаю нарушения требований ИБ должно приниматься решение о наложении на виновных лиц дисциплинарных взысканий.

8.12.2 В Учреждении должна быть разработана и утверждена формальная процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

8.12.3 Все работники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях.

8.12.4 Вопросы управления инцидентами ИБ должны регламентироваться отдельным внутренним документом Учреждения.

8.13 Обеспечение безопасности на этапах жизненного цикла ИС

8.13.1 Разработка, приобретение, а также внесение изменений (модернизация) в существующие элементы ИС Учреждения и их сопровождение должно проводиться только после выполнения следующих требований:

- определения требований ИБ, предъявляемых к разрабатываемой, приобретаемой, а также эксплуатируемой ИС Учреждения или ее элементам, удовлетворяющих требованиям законодательства Российской Федерации, нормативных документов Росгидромета и внутренних документов Учреждения в области защиты информации, а также исключающих нарушение характеристик ИБ системы защиты информации Учреждения;
- создания отдельных сред и тестовых данных для тестирования изменений, вносимых в ИС;
- применения мер ИБ на всех этапах жизненного цикла ИС.

8.13.2 Требования безопасности должны обосновываться и документально оформляться в рамках общего проекта по внедрению ИС.

8.13.3 Вопросы обеспечения безопасности на этапах жизненного цикла ИС должны регламентироваться отдельным внутренним документом Учреждения.

8.14 Использование АРМ и ИС

8.14.1 К работе в ИС Учреждения допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.

8.14.2 Каждому сотруднику Учреждения, которому необходим доступ к ИС в рамках его должностных обязанностей, выдаются под роспись необходимые средства автоматизации и организовывается автоматизированное рабочее место (АРМ). Ответственность по установке и поддержке всех ИС, включая АРМ, функционирующих в Учреждении, должна быть возложена на соответствующее структурное подразделение (лицо).

8.14.3 Все АРМ, установленные в Учреждении, должны иметь унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией, определённый в стандарте рабочих мест Учреждения. Изменение установленной конфигурации возможно после внесения соответствующих поправок в стандарт рабочих мест или по служебной записке.

8.14.4 Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется ответственным структурным подразделением (лицом) в соответствии со стандартом рабочих мест.

8.15 Использование ПО

8.15.1 На АРМ Учреждения допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения.

8.15.2 Запрещено незаконное хранение на жестких дисках АРМ Учреждения информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

8.15.3 Решение о приобретении и установке программного обеспечения, необходимого для реализации задач Учреждения принимает генеральный директор по представлению начальников отделов.

8.16 Управление изменениями

8.16.1 В Учреждении должен быть организован процесс управления изменениями. Все изменения, вносимые в программное обеспечение ИС и оборудование, должны регистрироваться и контролироваться.

8.16.2 Самостоятельная установка программного обеспечения на АРМ запрещена. Установка и удаление любого программного обеспечения производится только ответственным структурным подразделением (лицом).

8.16.3 Должны быть определены и зафиксированы параметры безопасных конфигураций ИС и оборудования. Данные параметры должны в обязательном порядке применяться при настройке и восстановлении работоспособности оборудования и ИС.

8.16.4 Вопросы управления изменениями должны регламентироваться отдельным внутренним документом Учреждения.

8.17 Использование информационных ресурсов

8.17.1 Для выполнения своих служебных обязанностей работники Учреждения обеспечиваются доступом к соответствующим информационным ресурсам.

8.17.2 Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Учреждения, базы данных, электронная почта.

8.17.3 Основными рабочими каталогами являются личные каталоги работников и каталоги подразделений, созданные в соответствии с особенностями их работы. Расширение прав доступа осуществляется ответственным структурным подразделением (лицом) в соответствии с Порядком предоставления (изменения) полномочий пользователя.

8.18 Резервное копирование и восстановление информации

8.18.1 В Учреждении должно выполняться регулярное резервное копирование информации, программного обеспечения и образов ИС.

8.18.2 Создаваемые резервные копии должны регулярно тестироваться. Должна быть обеспечена целостность создаваемых резервных копий.

8.18.3 Вопросы организации резервного копирования и восстановления информации должны регламентироваться отдельным внутренним документом Учреждения.

8.19 Управление непрерывностью деятельности

8.19.1 В Учреждении должен быть разработан и поддерживаться процесс обеспечения непрерывности обмена информацией и доступа к информационным активам в масштабах всего Учреждения, учитывающий требования Политики и внутренних документов по ИБ Учреждения, включающий в себя меры по выявлению и снижению рисков отказов и блокирования элементов ИС, ограничению последствий отказов ИС или аварий, и обеспечивающий доступность информационных активов, в том числе возможность их оперативного восстановления, требуемую для подержания

непрерывности деятельности Учреждения.

8.19.2 Принятые меры по обеспечению непрерывности деятельности должны быть отражены в разрабатываемом Плане обеспечения непрерывности и восстановления деятельности (далее – План).

8.19.3 План должен подвергаться проверке на регулярной основе. По результатам проверки в случае необходимости должен осуществляться пересмотр данного Плана.

8.20 Обеспечение безопасности при работе с персоналом

8.20.1 С целью снижения риска субъективных ошибок, краж, мошенничества или производственных злоупотреблений при приеме кандидатов на работу в Учреждении должны выполняться процедуры оценки благонадежности кандидатов на работу.

8.20.2 Должно осуществляться выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности работников, в том числе должен проводиться вводный инструктаж по ИБ для работников при приеме на работу, а также дальнейший контроль (проверка) полученных знаний. Должен быть разработан и доведен до сведения персонала порядок принятия дисциплинарных взысканий к тем работникам, которые допустили нарушение установленных требований ИБ.

8.20.3 Должна быть определена и доведена до сведения работников область их ответственности в части выполнения обязанностей по обеспечению ИБ, остающихся в силе после прекращения или изменения трудовых отношений с Учреждением.

8.21 Повышение осведомленности в области ИБ

8.21.1 В Учреждении должно осуществляться обучение и повышение осведомленности работников в области обеспечения ИБ.

8.21.2 Должны проводиться регулярные обучающие мероприятия для работников Учреждения. По результатам проведенных мероприятий должны проводиться регулярные проверки полученных знаний.

8.21.3 Вопросы повышения осведомленности должны регламентироваться отдельным внутренним документом Учреждения.

8.22 Обеспечение безопасности при взаимодействии с третьими лицами

8.22.1 Меры безопасности при организации работ с третьими лицами и сторонними организациями должны предусматривать:

– осуществление допуска сторонних организаций и третьих лиц к информационным активам Учреждения только после определения и реализации необходимых требований безопасности и ответственности за их нарушение, а также

включения таких требований в заключенные с указанными лицами и организациями договоры и соглашения;

– постоянный контроль доступа третьих лиц и сторонних организаций к информационным активам Учреждения и средствам ее обработки.

8.22.2 Вопросы обеспечения ИБ при взаимодействии с третьими лицами должны регламентироваться отдельным внутренним документом Учреждения.

8.23 Организация физической защиты

8.23.1 С целью предотвращения несанкционированного доступа, повреждения оборудования, вторжения в здания и помещения Учреждения должны быть выделены зоны (области) безопасности (в том числе особо важные и выделенные помещения), в которых должен поддерживаться режим физической безопасности.

8.23.2 В зонах безопасности, а также во всех офисных, вспомогательных, подсобных, технических и т.п. помещениях должны быть реализованы меры по противопожарной защите, защите от аварий в системах электро-, тепло-, водо-, газоснабжения, канализации и стихийных бедствий.

8.23.3 Посторонние лица, имеющие право на доступ в помещения Учреждения, должны регистрироваться, должен осуществляться контроль доступа в помещения (в том числе с использованием СКУД).

8.23.4 Посторонние лица должны допускаться в помещения только под контролем и в сопровождении ответственных работников Учреждения.

8.23.5 Для всех помещений должен быть назначен ответственный (распорядитель доступа). Доступ в помещения должен предоставляться только по согласованию с ответственным за помещение.

8.23.6 Входные двери помещений должны быть оборудованы механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время.

8.23.7 Серверное и сетевое оборудование ИС должно быть расположено в запираемых серверных стоечных шкафах. Доступ к данным шкафам должен быть под контролем.

8.23.8 В случае применения средств видеонаблюдения видеозаписи должны храниться не менее 14 (четырнадцати) календарных дней.

8.23.9 Вопросы организации физической защиты должны регламентироваться отдельным внутренним документом Учреждения.

8.24 Применение технических средств защиты информации

8.24.1 Технические средства защиты информации перед их использованием должны быть размещены в информационной инфраструктуре Учреждения и настроены

(сконфигурированы) в соответствии с требованиями эксплуатационной документации.

8.24.2 Для всех применяемых технических средств защиты информации должны быть обеспечена возможность их поддержки (сопровождения) в течение всего срока использования.

8.24.3 В случае необходимости использования технических средств защиты информации для нейтрализации актуальных угроз безопасности информации в соответствии с Моделью угроз Учреждения, должны применяться средства, сертифицированные ФСТЭК России по требованиям безопасности.

9 Ответственность

9.1 Генеральный директор Учреждения при обеспечении ИБ в Учреждении несет ответственность за:

- утверждение Политики и внутренних документов Учреждения в части обеспечения ИБ;
- утверждение направлений развития ИБ в контексте снижения общих бизнес-рисков Учреждения;
- выделение финансовых и материальных средств, а также кадровых ресурсов для организации обеспечения ИБ;
- утверждение организационной структуры подразделения обеспечивающего ИБ Учреждения.

9.2 Заместитель генерального директора, отвечающий за обеспечение ИБ в Учреждении несет ответственность за:

- планирование, контроль, организацию и развитие мер обеспечения и управления ИБ в Учреждении.

9.3 Директора филиалов Учреждения при обеспечении ИБ в филиале несут ответственность за:

- назначение ответственного лица отвечающего за обеспечение ИБ в филиале;
- доведение требований по обеспечению ИБ до работников филиала;
- выполнение требований законодательства Российской Федерации, нормативных документов регуляторов в области ИБ и иных применимых требований в области ИБ;
- своевременное информирование структурного подразделения, обеспечивающего ИБ Учреждения о выявленных рисках и инцидентах ИБ;
- организацию исполнения требований структурного подразделения, обеспечивающего ИБ Учреждения по минимизации последствий от возникновения рисков ИБ, устранению условий и последствий инцидентов.

9.4 Структурное подразделение (лицо) Учреждения, обеспечивающее ИБ несет

ответственность за:

- разработку, документирование и внедрение мер обеспечения и управления ИБ;
- определение мер, необходимых для реализации планов и стратегий в части управления и защиты информации на каждом этапе ее обработки;
- анализ угроз и рисков ИБ, планирование и реализация мероприятий по снижению угроз и управлению рисками, согласование бюджета мероприятий перед руководством Учреждения;
- выполнение требований законодательства Российской Федерации, нормативных документов регуляторов в области ИБ и иных применимых требований в области ИБ;
- контроль за применяемыми мерами ИБ и улучшение (совершенствование) применяемых мер;
- организацию обучения и повышения осведомленности работников в области ИБ.

9.5 Структурное подразделение (лицо) Учреждения, отвечающее за техническую поддержку, при обеспечении ИБ в Учреждении несет ответственность за:

- поддержку и участие в процессах обеспечения ИБ, связанных с использованием ИС и АРМ;
- соблюдение установленных требований в части обеспечения ИБ при разработке, внедрении и эксплуатации ИС и информационных активов;
- участие в процессе анализа угроз и рисков ИБ, планирование и реализацию мероприятий по снижению угроз и управлению рисками совместно со структурным подразделением, обеспечивающим информационную безопасность;
- планирование, реализацию мероприятий, направленных на сопровождение закупок, эксплуатацию ИС и АРМ в целях ИБ;
- управление применяемыми техническими средствами защиты информации, а также их сопровождение;
- предоставление информации о применяемых информационных технологиях и ИС Управлению информационной безопасности.

9.6 Руководители структурных подразделений Учреждения при обеспечении ИБ в Учреждении несут ответственность за:

- управление информационными активами, согласование прав доступа к информационным активам, принятие решений по рискам нарушения ИБ, связанным с информационными активами, находящимися в зоне ответственности структурного подразделения;
- доведение требований по обеспечению ИБ до работников подчиненных структурных подразделений;

- своевременное информирование структурного подразделения, обеспечивающего ИБ о выявленных рисках и инцидентах ИБ;
- исполнение требований структурного подразделения, обеспечивающего ИБ по минимизации последствий от возникновения рисков ИБ, устранению условий и последствий инцидентов.

9.7 Работники Учреждения, в том числе филиалов при обеспечении ИБ несут ответственность за:

- исполнение требований внутренних документов Учреждения в части обеспечения ИБ.

9.8 Политика должна быть доведена до всех работников и принята ими к обязательному исполнению. Политика также должна быть доведена до контрагентов и иных третьих лиц, допущенных к информационным активам Учреждения, и принята ими к обязательному исполнению в части, их касающейся.

9.9 Все работники Учреждения, а также иные третьи лица при обращении с информационными активами Учреждения должны руководствоваться утвержденными требованиями организационно-распорядительных, эксплуатационных, методических и иных документов, связанных с обеспечением ИБ, в том числе требованиями Политики.

9.10 За нарушение требований в области ИБ работники Учреждения несут персональную ответственность в соответствии с законодательством Российской Федерации.

9.11 Ответственность за осуществление общего контроля выполнения Политики, предоставление рекомендаций по их выполнению, поддержание Политики в актуальном состоянии с учетом требований международных и национальных стандартов, а также законодательства Российской Федерации, нормативных документов Росгидромета и регуляторов в области ИБ, несет заместитель генерального директора Учреждения, ответственный за обеспечение информационной безопасности.

10Лист регистрации изменений

Политика информационной безопасности ФГБУ «Авиаметтелеком Росгидромета»								
Номер изменения	Номер страницы				Дата и номер приказа об изменении и номер пункта в приказе	Подпись	Дата	
	изме-ненной	заме-ненной	новой	анну-лиро-ванной			внесе-ния	введения

11Лист регистрации ознакомлений

Политика информационной безопасности ФГБУ «Авиаметтелеком Росгидромета»				
№ п/п	Дата	Дата и номер приказа об изменении	ФИО	Подпись
1	2	3	4	5

28 об