Утверждено
Приказом КГСАУ «ДВ авиабаза»
«Об утверждении Политики
обеспечения безопасности
информации в автоматизированной
информационной системе
КГСАУ «ДВ авиабаза»

ПОЛИТИКА
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ (**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**)

в краевом государственном специализированном автономном учреждении
«Дальневосточная база авиационной охраны лесов»
(КГСАУ «ДВ авиабаза»)

г. Хабаровск 2026 года

Приняты следующие основные термины, определения и сокращения, используемые в данном документе и в иных документах, регламентирующих информационную безопасность:

Учреждение	Краевое государственное специализированное автономное учреждение «Дальневосточная база авиационной охраны лесов» или сокращенно КГСАУ «ДВ авиабаза»
АРМ	Автоматизированное рабочее место
АИС	Автоматизированная информационная система, включающая в себя локально-вычислительною сеть и телекоммуникационную систему Учреждения
Информационные ресурсы	отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).
Классификация информационных ресурсов	*По целевому предназначению*: личные, корпоративные, СМИ, бизнес, образовательные, политика, учреждения и организации, сервисы и услуги, доски объявлений, культура, чаты, хранилища ПО, спорт, отдых, изображения и фото, развлекательные порталы.
	По способу представления: Web-страницы; Базы данных; Файловые серверы; Телеконференции.
	По национально-территориальному признаку: - по языковому признаку. - по географическому признаку.
	По режиму доступа: открытая информация (без ограничения); информация ограниченного доступа; конфиденциальная информация; коммерческая тайна; профессиональная тайна; личная (персональная) тайна.
	По форме собственности: общероссийское национальное достояние; государственная собственность; собственность субъектов РФ; муниципальная собственность; частная (личная, корпоративная) собственность.
	По способу организации хранения и использования: традиционные формы (книги, газеты, журналы); массив документов; фонд документов; архив; автоматизированные формы.
	По виду носителя: твердая копия (книга, газета, рукопись и т.д.); на машиночитаемых носителях (к/пленка, аудио- и видеозапись, данные на винчестере компьютера, дискете, CD и т.д.); на канале связи (TV, R).
	По характеру содержания: Тематическая информация; Научные публикации; Рекламная информация; Справочная информация; Новости; Вторичная информация.
Безопасность информации	состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами
Доступ к информации	возможность получения информации и ее использования
Доступность информации	состояние информации, характеризуемое способностью АИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия
Защита информации от несанкционированного доступа	деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию)
Защищенные помещения	помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.)
Информативный сигнал	электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах или обсуждаемая в защищенных помещениях

Информационные сети общего пользования (Сети)	вычислительные (информационно-телекоммуникационные) сети, открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано
Контролируемая зона (КЗ)	это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание работников и посетителей организации, а также транспортных средств. Границей КЗ могут являться: - периметр охраняемой территории организации; - ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.
Конфиденциальная информация	информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации
Конфиденциальность информации	состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней
Межсетевой экран (МЭ)	локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АИС и (или) выходящей из АИС. МЭ обеспечивает защиту АИС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АИС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АИС к объектам другой АИС.
Локальная вычислительная сеть (ЛВС)	совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с другими информационно-телекоммуникационными системами, в том числе с ЛВС, через определенные точки входа/выхода информации, которые являются границей ЛВС
Несанкционированный доступ (НСД)	доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АИС.
Роли информационной безопасности	согласованные обязанности, права и ответственность по классификации, инвентаризации, определению угроз и рисков, распоряжению, защите, использованию, контролю, администрированию и обслуживанию информационных ресурсов Учреждения. Роли определяются и назначаются работникам Учреждения для каждого информационного ресурса.
Сегменты локальной вычислительной сети (ЛВС)	составные части локальной вычислительной сети (ЛВС): внутренние, закрытые, удаленные, демилитаризованные зоны (DMZ). Внутренние - сегменты, в которых размещаются рабочие станции и серверное оборудование. Закрытые - специально выделенные, как правило, за счет применения устройств маршрутизации, участки внутренней сети, не имеющие соединений с ее внешними устройствами. Удаленные сегменты, подключаемые к основным участкам сети с ПОМОЩЬЮ различных средств связи. Демилитаризованные зоны отделяют общедоступное серверное оборудование от внутренней сети и обеспечивают возможность обнаружения вторжений, контроль трафика, а также дополнительный уровень защиты ЛВС
Система защиты информации от НСД	комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации (несанкционированных действий с ней) в АИС.
Технический канал утечки информации	совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.
Техническая защита конфиденциальной информации (ТЗКИ)	защита информации не криптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения или блокирования.

Целостность информации	состояние защищенности информации, характеризуемое способностью АИС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.
Структурное подразделение	подразделения административно управленческого аппарата КГСАУ «ДВ авиабаза» г. Хабаровск и авиабазы.

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Настоящая Политика обеспечения информационной безопасности в автоматизированной информационной системе КГСАУ «ДВ авиабаза» (далее - Политика) разработана в рамках реализации требований:

- Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона №152-ФЗ «О персональных данных»;
- Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Инструкции по делопроизводству, утвержденной Приказом № 01-05-52 от 28.08.2025.

1.2. Является локальным нормативным актом, устанавливающим основные принципы, порядок и правила обеспечения информационной безопасности в автоматизированной информационной системе Учреждения, а также основным документом, регламентирующим деятельность Учреждения в области обеспечения безопасности информационных технологий и информационных ресурсов.

1.3. Политика разработана в целях установления общих норм и правил защиты информационных ресурсов от внешних и внутренних угроз, информирования пользователей об обязательных требованиях по защите информационных технологий и информационных ресурсов.

1.4. Под Политикой понимается совокупность документированных управленческих решений, направленных на защиту информационных технологий и информационных ресурсов, регламентирующих эффективную работу средств защиты информации и определяющих поведение информационных систем и ее пользователей в различных ситуациях.

1.5. Политика реализуется посредством локальных нормативных, организационных, технических и режимных мер.

1.6. Требования Политики распространяются на работников Учреждения.

1.7. Политика рекомендована для применения путем включения ссылок на нее и (или) прямого использования устанавливаемых в ней положений в локальных нормативных и методических документах Учреждения.

1.6. Актуализация Политики производится:

1.6.1. при внесении существенных изменений в конфигурацию и условия эксплуатации автоматизированных информационных систем (АИС);

1.6.2. при изменении законодательства Российской Федерации в области информационной безопасности;

1.6.3. при происшествиях и инцидентах, связанных с нарушением информационной безопасности, повлекших нанесение ущерба Учреждению.

2. ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

2.1. Основными объектами обеспечения информационной безопасности являются:

2.1.1. информационные ресурсы, содержащие сведения конфиденциального характера, а также подлежащая защите открытая информация (в дальнейшем - защищаемая информация или защищаемый информационный ресурс);

2.1.2. средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), с использованием которых осуществляется обработка, передача и хранение защищаемой информации;

2.1.3. программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), с использованием которых осуществляется обработка защищаемой информации;

2.1.4. помещения, предназначенные для проведения мероприятий, в ходе которых обсуждается защищаемая информация, и помещения, в которых размещены средства обработки защищаемой информации (защищаемые помещения);

2.1.5. технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация;

2.1.6. серверные и вспомогательные помещения.

2.2. Защищаемая информация может:

2.2.1. обрабатываться и храниться на бумажных носителях;

2.2.2. обрабатываться, передаваться и храниться с использованием средств вычислительной техники, связи и автоматизации в электронном виде;

2.2.3. передаваться по каналам передачи данных (в том числе по телефону, видеоконференцсвязи и т.п.) в виде электрических сигналов;

2.2.4. присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;
2.2.5. записываться и воспроизводиться с помощью технических средств.

3. ЗАЩИЩАЕМЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ.

3.1. Конфиденциальные сведения - информация, определенная Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

3.3. Коммерческая тайна - информация, подпадающая под действие Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и определенная п.10 Инструкции по делопроизводству.

3.4. Персональные данные - информация, подпадающая под действие Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.5. Публичная информация - информация о деятельности Учреждения, предназначенная для представления в публичный доступ и размещения на внешних публичных ресурсах Учреждения (публичный www-сервер - http://airbase.khv.ru).

3.6. Открытая информация, сформированная в результате операционной деятельности Учреждения и имеющая ключевое значение для обеспечения функционирования производственной, финансовой и хозяйственной деятельностей.

4. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

4.1. Под угрозами информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию. К основным угрозам информационной безопасности относятся:
4.1.1. утечка защищаемой информации - несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, разглашение, копирование, хищение и т.д.), утечка информации по каналам связи и за счет побочных электромагнитных излучений;
4.1.2. недоступность защищаемой информации - блокирование информационных ресурсов, сбои в работе технических средств или программного обеспечения, дезорганизация функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления базами данных, распределенных информационных сетей, воздействие вредоносного программного обеспечения, стихийных бедствий и иных форс-мажорных обстоятельств;

4.1.3. потеря защищаемой информации уничтожение, искажение (несанкционированная модификация, подделка) информационных ресурсов.

4.2. Источниками возникновения угроз информационной безопасности являются:
4.2.1. непреднамеренные угрозы - недостаточная квалификация работников, несовершенство программного обеспечения и технических средств, чрезвычайные ситуации природного и техногенного характера, действия работников, не преследующие корыстных целей, но приводящие к непредвиденным негативным последствиям;
4.2.2. преднамеренные угрозы - действия конкурентов, контрагентов, клиентов, действия иных злоумышленников, в том числе из внутренней среды -персонала и их окружения (инсайдеры).

4.3. В результате воздействия угроз информационной безопасности существует вероятность возникновения следующих негативных последствий:
4.3.1. экономических (финансовые потери, связанные с утечкой защищаемой информации, с уничтожением и последующим восстановлением утраченной информации; ущерб от дезорганизации деятельности Учреждения и потери, связанные с невозможностью выполнения им своих обязательств);
4.3.2. интеллектуальных (ущерб от утери созданной, наработанной интеллектуальной собственности);
4.3.3. репутационных (ущерб репутации Учреждения, работников, руководителей и учредителя).

4.4. Критерии оценки возможных последствий реализации угроз информационной безопасности учитываются при принятии решения о защите конкретных информационных ресурсов.

5. ОСНОВНЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Локальные нормативные, правовые и организационные меры:
5.1.1. реализация требований Федерального закона № 187-ФЗ в части определения статуса объектов критической информационной инфраструктуры, установление ответственности за соблюдение требований правовых актов Российской федерации в сфере информационной безопасности;
5.1.2. разработка правил «Информационной безопасности», определяющих порядок защиты информационных ресурсов, периодическое уточнение и оценка эффективности принимаемых мер;
5.1.3. включение обязанностей и ответственности в области обеспечения информационной безопасности в положениях о структурных подразделениях и в должностных инструкциях работников Учреждения;

5.1.4. проведение вводных инструктажей при приеме на работу, переводе в другое подразделение, проведение обучения работников по вопросам обеспечения информационной безопасности, подготовка и повышение квалификации специалистов осуществляющие администрирование информационных ресурсов Учреждения;
5.1.5. разработка правил (регламентов, инструкций) эксплуатации технических и программных средств с учетом требований информационной безопасности;
5.1.6. разработка регламентов работы с документами, содержащими конфиденциальные сведения;
5.1.7. разработка и совершенствование нормативно-правовой базы, регламентирующей порядок обмена информационными ресурсами между Учреждением и сторонними организациями;
5.1.8. обеспечение принципа разграничения доступа к защищаемым информационным ресурсам с учетом минимально достаточных прав по доступу к информации, необходимой для выполнения работниками своих должностных обязанностей;
5.1.9. использование информационных ресурсов, в том числе сети «Интернет» и электронной почты, только в служебных целях.

5.2. Технические меры:
5.2.1. использование лицензионного программного обеспечения, свободно распространяемого программного обеспечения, прошедшего этап опытной эксплуатации;
5.2.2. обеспечение безотказности работы аппаратных средств, с учетом дублирующих функций;
5.2.3. реализация комплексной защиты от вредоносного программного обеспечения, с использованием, как внутренних программных возможностей, так и стороннего антивирусного обеспечения;
5.2.4. реализация эффективной парольной защиты;
5.2.5. реализация резервного копирования информации и обеспечение процедур резервного копирования и восстановления;
5.2.6. использование межсетевых экранов на стыке внутренних (локальных) и внешних сетей;
5.2.6. создание виртуальных частных сетей для защищенного обмена информацией между распределенными сегментами информационных систем;
5.2.7. использование единой базовой системы авторизации (предоставление прав) пользователей и разграничения прав доступа к ресурсам АИС;
5.2.8. создание системы обнаружения вторжений из внешних сетей и из локальной сети;

5.2.9. использование инфраструктуры открытых ключей (PKI) для обеспечения единой многофакторной аутентификации (подтверждения заявленной личности) пользователей и применения криптографических средств защиты информации;
5.2.10. использование актуальных обновлений для средств защиты информации, операционных систем и прикладного программного обеспечения;
5.2.11. запрет несанкционированного доступа через удаленные соединения;
5.2.12. проводить ежеквартальный аудит систем защиты информации;
5.2.13. проводить ежеквартальный аудит прав доступа пользователей АИС.

5.3. Режимные меры:
5.3.1. хранение, обработка и обмен электронной информацией, содержащей конфиденциальные сведения, только с применением сертифицированных средств защиты информации, в том числе криптографических;
5.3.2. ограничение круга лиц, имеющих право работы со сведениями конфиденциального характера;
5.3.3. установление специальных режимных мер, применяемых в целях информационной безопасности (ведение конфиденциального делопроизводства, выделение и контроль состояния безопасности специально оборудованных помещений, поддержание необходимого уровня пропускного и внутриобъектового режимов, подбор кадров, проведение комплексных защитно-поисковых мероприятий и т.п.);
5.3.4. разграничение и контроль доступа в защищаемые помещения;
5.3.5. реализация системы контроля выполнения работниками Учреждения требований локальных нормативных актов по обеспечению информационной безопасности.

5.4. Основными направлениями защиты конфиденциальной информации являются:
5.4.1. обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет несанкционированных действий;
5.4.2. обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

5.5. В качестве основных мер защиты конфиденциальной информации, с учетом перечисленных выше, предусматривается:
5.5.1. документальное оформление перечня сведений, содержащих конфиденциальную информацию;
5.5.2. регистрация действий и контроля доступа пользователей АИС Учреждения;

5.5.3. учет и надежное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение;
5.5.4. использование сертифицированных серийно выпускаемых в защищенном исполнении технических средств обработки, передачи и хранения информации;
5.5.5. использование сертифицированных средств защиты информации;
5.5.6. использование защищенных каналов связи;
5.5.7. размещение экранов мониторов и других средств отображения информации, исключающих несанкционированный просмотр;
5.5.8. предотвращение внедрения в информационные системы программ-вирусов, программных закладок и др.

5.6. Проводить дифференцированный подход к защите информации, обрабатываемой в АИС различного уровня и назначения с учетом используемых и прогнозируемых финансовых затрат.

5.7. Лица, допущенные к автоматизированной обработке конфиденциальной информации, несут ответственность за соблюдение ими установленного законодательством Российской Федерации, а также локальными нормативными актами Учреждения порядка обеспечения ее защиты.

6. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Система обеспечения информационной безопасности создается на основе разграничения управленческих и функциональных полномочий подразделений Учреждения в сфере информационной безопасности. Основными субъектами системы обеспечения информационной безопасности являются:
6.1.1. Начальник учреждения;
6.1.2. Заместитель начальника учреждения;
6.1.3. отдел кадров;
6.1.4. руководители структурных подразделений;
6.1.5. специалисты ответственные за администрирование информационных сетей и ресурсов.
6.2. Начальник учреждения определяет приоритетные направления деятельности в области обеспечения информационной безопасности и меры по реализации Политики. Утверждает руководящие документы, правила, регламенты, инструкции, а также перечни сведений, подлежащих защите.

6.3. Заместитель начальника учреждения с учетом определенных начальником учреждения приоритетных направлений в области обеспечения информационной безопасности осуществляет:
6.3.1. общее руководство проведением мероприятий по защите информации;
6.3.2. координирует деятельность структурных подразделений с учетом требований информационной безопасности Учреждения.

6.3.3. организует разработку и реализацию нормативно-правовых, организационных, технических и режимных мер по обеспечению информационной безопасности;
6.3.4. координирует деятельность подразделений Учреждения в области информационной безопасности.
6.4. Специалисты ответственные за администрирование информационных сетей и ресурсов:
6.4.1. проводит работу по выявлению и оценке угроз информационной безопасности, разрабатывает предложения по их предотвращению;
6.4.2. обеспечивает корректное и бесперебойное функционирование выделенных средств защиты информации;
6.4.3. контролирует состояние информационной безопасности;
6.4.4. обеспечивает организацию работы по классификации и инвентаризации информационных ресурсов;
6.4.5. выполняет организационные и технические меры по обеспечению информационной безопасности в ходе разработки, внедрения и функционирования автоматизированной информационной системы;
6.4.6. обеспечивает настройку, корректное и бесперебойное функционирование встроенных средств защиты;
6.4.7. согласует приобретение программных и аппаратных технических средств, предназначенных для использования в составе действующих и создаваемых АИС Учреждения.

6.5. Отдел кадров (специалист по делопроизводству) обеспечивает регистрацию и учет всех служебных документов и носителей конфиденциальной информации.

6.6. Руководители структурных подразделений Учреждения обеспечивают:
6.6.1. классификацию информационных ресурсов, находящихся в ведении структурных подразделений;
6.6.2. ведение реестров защищаемых информационных ресурсов;
6.6.3. выполнение работниками установленных требований в области обеспечения информационной безопасности.
6.7. Обеспечение информационной безопасности непосредственно на рабочих местах возлагается на работников Учреждения.

7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

7.1. Нарушения, связанные с невыполнением норм, правил и требований нормативных актов по обеспечению информационной безопасности Учреждения, по степени опасности делятся на две группы:

7.1.1. повлекшие за собой наступление нежелательных для Учреждения последствий (утечку, блокирование, уничтожение или модификацию защищаемой информации, как результат причинение материального ущерба, утери интеллектуальной собственности и нанесения вреда имиджу Учреждения);
7.1.2. в результате которых созданы предпосылки для наступления нежелательных для Учреждения последствий (угроза утечки, блокирования, уничтожения или модификации защищаемой информации, как результат угроза причинения материального ущерба, утери интеллектуальной собственности и нанесения вреда имиджу Учреждения);

7.2. Нарушение требований информационной безопасности влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами и трудовыми договорами, заключенными между Учреждением и работниками.

7.3. Степень ответственности за нарушение требований локальных нормативных актов в области информационной безопасности определяется, исходя из размера ущерба, причиненного Учреждению.

7.4. Руководители структурных подразделений несут персональную ответственность за обеспечение информационной безопасности в подведомственных им подразделениях.

7.5. Работники Учреждения несут персональную ответственность за обеспечение информационной безопасности непосредственно на своих рабочих местах.

КГСАУ «ДВ авиабаза»
редакция от 10 июля 2026 года на 12-ти листах

Права на данный документ принадлежат Учреждению. Документ не может быть полностью или частично воспроизведен, опубликован, тиражирован, скопирован или распространен в любой иной форме без разрешения Учреждения.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат dcb1a8bb63b7d0cd024380220d717901
Владелец Домрачев Егор Александрович
Действителен с 28.04.2025 по 22.07.2026