

УТВЕРЖДЕНА
приказом АК «АЛРОСА» (ПАО)
от «22» ноября 2024 г. № 01/325-П

ПОЛИТИКА
информационной безопасности Группы АЛРОСА

СОДЕРЖАНИЕ

Нормативные ссылки	3
Термины и определения.....	4
1. Общие положения и область действия.....	6
2. Цели, задачи и принципы обеспечения информационной безопасности	7
3. Система обеспечения информационной безопасности.....	8
4. Объекты защиты и меры обеспечения информационной безопасности.....	9
5. Структура внутренних нормативных документов	10
6. Ответственность	11

Нормативные ссылки

Настоящая Политика информационной безопасности Группы АЛРОСА разработана с учетом следующих нормативных актов:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Указ Президента Российской Федерации от 01 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- ГОСТ Р ИСО/МЭК 27001-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- ГОСТ Р ИСО/МЭК 9001-2015 «Системы менеджмента качества. Требования».

Термины и определения

В настоящей Политике информационной безопасности Группы АЛРОСА использованы следующие термины и определения:

Аудит информационной безопасности – систематический, независимый и документируемый процесс получения свидетельств деятельности по обеспечению информационной безопасности и установлению степени выполнения критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности.

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Бизнес-процесс – совокупность взаимосвязанных повторяемых технологических операций, направленных на получение определенного результата и преобразующих исходный материал и/или информацию в конечный продукт (услугу) в соответствии с предварительно установленными правилами.

Владелец информационного актива – работник или подразделение, которое уполномочено руководством организовывать и координировать по отношению к информационному активу процессы категорирования и использования, управления развитием и обслуживанием, принятия решений об остановке и выводе из эксплуатации, обеспечения безопасности с возможностью делегирования данных полномочий. Термин «владелец» не означает, что работник или подразделение обладает правами собственности на сам актив.

Группа АЛРОСА – АК «АЛРОСА» (ПАО) и ее дочерние общества.

Информационная безопасность (ИБ) – состояние защищенности технологических и бизнес-процессов, объединяющих в своем составе работников, технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере. Защищенность достигается обеспечением доступности, целостности и конфиденциальности информационных активов.

Информационный актив – сведения АК «АЛРОСА» (ПАО) и ее дочерних обществ, которые представляют ценность (финансовая информация, информация ограниченного доступа, сведения об информационной инфраструктуре и т.д.), а также корпоративная и технологическая сети передачи данных, включающие информационные системы, базы данных, технические и программные средства, каналы информационного обмена, средства защиты информации, средства криптографической защиты информации, помещения, автоматизированные системы управления.

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами или внутренними нормативными документами АК «АЛРОСА» (ПАО) и её дочерних обществ.

Инцидент информационной безопасности – появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ.

Объекты критической информационной инфраструктуры (КИИ) – объекты критической информационной инфраструктуры, в том числе значимые, а именно: информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления;

Киберучения – мероприятия по моделированию атак, в рамках которых проверяются актуальность и работоспособность процедур выявления атак, а также эффективность имеющихся планов, схем реагирования и мер по ликвидации последствий.

Конфиденциальность – свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов.

Корпоративная сеть передачи данных (КСПД) – сеть АК «АЛРОСА» (ПАО), в которой циркулирует информация, формирующая единое внутреннее информационное пространство и обеспечивающая доступ к корпоративным ИТ-сервисам.

Риск информационной безопасности – потенциальные возможности использования уязвимостей информационного актива или группы активов конкретной угрозой для причинения ущерба.

Система информационной безопасности (СИБ) – совокупность защитных мер и средств, включая ресурсное и административное (организационное) обеспечение.

Система управления информационной безопасностью (СУИБ) – часть менеджмента, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения информационной безопасности.

Система обеспечения информационной безопасности – совокупность СИБ и СУИБ.

Средства защиты информации (СЗИ) – совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Средства криптографической защиты информации (СКЗИ) – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

Событие информационной безопасности – идентифицированное появление определенного состояния информационного актива, указывающего на возможное нарушение внутренних нормативных документов по информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к информационной безопасности.

Технологическая сеть передачи данных (ТСПД) – сеть связи, используемая для оперативного управления технологическими процессами, передачи телеметрии и оповещения.

Угроза информационной безопасности – совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающих или способных вызвать негативные последствия (ущерб/вред).

Частная политика информационной безопасности – внутренний нормативный документ, детализирующий положения Политики информационной безопасности применительно к одной или нескольким областям информационной безопасности, видам и технологиям деятельности.

1. Общие положения и область действия

1.1. Настоящая Политика информационной безопасности Группы АЛРОСА (далее – Политика) разработана в соответствии с законодательством Российской Федерации, рекомендациями лучших российских и международных практик в части обеспечения информационной безопасности (далее – ИБ), требованиями нормативных актов Российской Федерации, уполномоченных органов исполнительной власти.

1.2. Целями настоящей Политики являются:

- закрепление целей и задач, которые ставит перед собой АК «АЛРОСА» (ПАО) (далее – Компания) и ее дочерние общества (далее – ДО) в области обеспечения ИБ;
- декларация основных принципов ИБ, которыми руководствуется Компания и ее ДО;
- описание состава и структуры системы обеспечения ИБ Компании и ее ДО, а также функций и ее участников;
- формирование понимания работниками Компании и ее ДО основных процессов и роли ИБ в деятельности Компании и ее ДО;
- описание основных организационно-технических подходов и мероприятий обеспечения ИБ Компании и ее ДО;
- определение структуры внутренних нормативных документов (далее – ВНД) Компании и ее ДО по ИБ.

1.3. ВНД Компании и ее ДО не должны противоречить настоящей Политике.

1.4. Политика является верхнеуровневым документом для действующих и вновь разрабатываемых ВНД по ИБ (частные политики, положения, методики, процедуры, регламенты, инструкции), детализирующих положения настоящей Политики и раскрывающих подробности реализации отдельных мероприятий по обеспечению ИБ.

1.5. Политика является методологической основой для:

- формирования и проведения единых принципов в области обеспечения ИБ;
- разработки мер по снижению рисков и угроз ИБ для бизнес-процессов Компании и ее ДО;
- применения единых принципов обеспечения ИБ при создании, развитии и эксплуатации КСПД, ТСПД, информационных систем и автоматизированных систем управления;
- разработки иных документов по ИБ, описывающих комплекс организационно-технических мер, направленных на своевременное выявление, предотвращение и ликвидацию последствий реализации различных видов угроз.

1.6. Положения настоящей Политики распространяются на все бизнес-процессы Компании и ее ДО, ее информационные активы (системы, инфраструктуру и т.д.) и являются обязательными для выполнения всеми работниками Компании и ее ДО, а также распространяются на взаимоотношения с поставщиками, провайдерами и иными партнерами, услуги которых связаны с использованием, обработкой или доступом к информации или информационным активам Компании и ее ДО.

1.7. Дочерние общества Компании присоединяются к настоящему документу путем принятия уполномоченным органом управления дочернего общества решения о присоединении к документу Компании.

2. Цели, задачи и принципы обеспечения информационной безопасности

2.1. Руководство Компании и её ДО осознает важность и необходимость совершенствования мер и средств обеспечения ИБ в контексте возрастания внешних угроз, развития законодательства, ожиданий клиентов Компании и её ДО и других заинтересованных сторон.

2.2. Целями обеспечения ИБ в Компании и ее ДО являются:

- обеспечение штатного функционирования и устойчивого развития Компании и ее ДО в условиях существующих угроз ИБ, а также предотвращение и/или снижение ущерба от инцидентов применением адекватных мер защиты;
- повышение доверия к Компании и ее ДО со стороны работников, клиентов, партнеров и формирование положительной репутации и имиджа Компании;
- выполнение требований законодательства.

2.3. Для достижения целей необходимо решение следующих основных задач:

- формирование единой политики ИБ и методологических подходов в Компании и ее ДО;
- построение эшелонированной защиты с полным покрытием информационных активов Компании и ее ДО;
- построение проактивной системы защиты с непрерывным мониторингом (24/7) событий ИБ для своевременного выявления, предотвращения и обработки инцидентов ИБ;
- выявление потенциальных угроз ИБ и выработка адекватных мер противодействия (риск-ориентированный подход);
- выполнение требований законодательства в области ИБ;
- обучение, повышение осведомленности и внедрение культуры ИБ в повседневную деятельность работников.

2.4. Компания и её ДО придерживаются следующих основных принципов ИБ:

- **разумной достаточности (сбалансированности защиты)** – предпочтения отдаются организационным и техническим мерам ИБ, требующим минимальных вложений со стороны Компании и (или) её ДО, при достижении необходимого и достаточного уровня защиты. Компания и её ДО придерживаются внедрения риск-ориентированного подхода внедрения ИБ. Проработка соотношения «цена-качество» при выборе инструментов ИБ, в т.ч. по опыту апробаций в аналогичных организациях. Фокус на изменения, не требующие опережающего роста затрат и штата;
- **непрерывности обеспечения ИБ (мониторинга и реагирования)** – организация процессов непрерывного (24/7) обнаружения и реагирования на инциденты ИБ для минимизации возможного ущерба;
- **прозрачности и адаптивности** – мониторинг и прозрачность прогресса реализации инициатив ИБ внутри функции ИБ и для менеджмента Компании и её ДО, синхронизация с бизнес-приоритетами;
- **комплексности и системности (полное и эшелонированное покрытие информационной инфраструктуры с учетом всех связей)** – обеспечение ИБ всего комплекса информационных активов Компании и ее ДО. Применение комплекса средств на различных уровнях информационной инфраструктуры для совокупного снижения рисков ИБ;

– **подтверждения результата** – проверяемость и возможность объективного подтверждения эффективности внедрения мер и средств ИБ различными путями: внутренний и внешний аудит ИБ, тестирование на проникновение и/или киберучения и т.д.;

– **законности (комплаенс)** – вся деятельность по обеспечению ИБ должна осуществляться при строгом соблюдении действующего законодательства Российской Федерации и требований регуляторов;

– **приоритета мер предупреждения (проактивная защита)** – деятельность по обеспечению ИБ должна носить упреждающий характер. Выбор мер ИБ должен осуществляться с учётом возможности появления принципиально новых сценариев реализации угроз ИБ, предполагать проактивные меры противодействия им.

3. Система обеспечения информационной безопасности

3.1. В Компании внедрена система менеджмента качества, основанная на требованиях международного стандарта ISO 9000. Одним из принципов обеспечения системы менеджмента качества является внедрение процессного подхода.

3.2. Система обеспечения информационной безопасности (далее – СОИБ) Компании должна функционировать в соответствии с серией стандартов ISO 27000 (аналог ISO 9000 для ИБ) и представляет собой цикл Шухарта-Деминга, включающий четыре группы процессов: «планирование – реализация – проверка – совершенствование».

3.3. Структура и состав СОИБ Компании и её ДО представлены на рисунке 1.



Рисунок 1. СОИБ Компании

3.4. **Система ИБ** Группы АЛРОСА состоит из совокупности защитных мер, реализующих процессы обеспечения ИБ, включая их ресурсное и организационное обеспечение.

3.5. **Система управления ИБ** Группы АЛРОСА состоит из совокупности процессов управления ИБ, включая их ресурсное и организационное обеспечение.

3.6. Группа процессов «планирование» включает в себя разработку стратегических и оперативных планов по повышению уровня ИБ в соответствии с растущими потребностями бизнеса, усложняющейся информационной инфраструктурой и появлением новых технологий, продуктов, услуг, а также изменениями в законодательстве.

3.7. Группа процессов «реализация» включает в себя деятельность по выполнению текущих и стратегических задач по обеспечению ИБ.

3.8. Группа процессов «проверка» включает в себя контрольные процедуры по определению уровня соответствия ИБ Компании и её ДО требованиям законодательства. Соответствие уровня ИБ осуществляется следующими способами:

- самооценкой работниками Компании и её ДО без привлечения внешних организаций;
- внутренним аудитом;
- аудитом внешними организациями;
- аудитом в рамках государственного контроля.

3.9. Аудит может проводиться в форме плановых и внеплановых проверок.

3.10. Группа процессов «совершенствование» включает внесение изменений в цели, планы, мероприятия и ВНД Компании в соответствии с результатами, полученными на этапе «проверка».

4. Объекты защиты и меры обеспечения информационной безопасности

4.1. Объектами защиты Компании и её ДО являются информационные активы. Обеспечение ИБ должно осуществляться в отношении всех информационных активов.

4.2. Компания и ее отдельные дочерние общества являются субъектами критической информационной инфраструктуры Российской Федерации и операторами персональных данных.

4.3. В отношении каждого информационного актива Компании и ее ДО на этапе ввода в промышленную эксплуатацию назначается его владелец. Владелец информационного актива несет ответственность за принятие решений об использовании, остановке и выводе из эксплуатации информационного актива, контролирует предоставление и отзыв прав доступа к активу и несет ответственность за предоставление избыточного объема прав.

4.4. Информационные активы Компании и ее ДО должны быть категоризованы. Правила категоризовывания устанавливаются действующим законодательством Российской Федерации и ВНД Компании.

4.5. Для обеспечения безопасности объектов защиты применяются следующие меры:

- **организационные** – система ВНД, состоящая из настоящей Политики, частных политик, методик, регламентов, инструкций и т.д.;

– **технические** – реализуемые при помощи средств защиты, штатных механизмов системного и прикладного программного обеспечения, коммутационного оборудования и т.п.

4.6. Меры защиты должны отвечать следующим основным требованиям:

- своевременное обнаружение и реагирование на инциденты достигается созданием единого центра мониторинга в режиме 24/7 покрытием всех информационных активов;
- обеспечение эшелонированной (многоуровневой) системы защиты;
- устранение известных уязвимостей и регулярный контроль их отсутствия;
- сегментирование сетей и контроль за сетевым и пользовательским доступом к информационным активам;
- разделение сред разработки, тестирования и продуктивных сред эксплуатации;
- применение СЗИ и СКЗИ в соответствии с актуальными угрозами ИБ;
- безопасная настройка и регулярный контроль параметров информационных систем, оборудования и программного обеспечения, оказывающих влияние на состояние ИБ;
- определение основных ролей и разделение функций по управлению (администрированию) информационными системами, управлению (администрированию) системами обеспечения ИБ, пользовательских функций по обработке данных и иных функций;
- обеспечение безопасной разработки ПО;
- минимизация полномочий – предоставление пользователям минимальных прав доступа в соответствии с исполняемой ими ролью и производственной необходимостью;
- обучение и повышение уровня осведомленности пользователей в сфере ИБ;
- расследование инцидентов и фактов нарушений в области ИБ с целью совершенствования принятых мер;
- анализ эффективности и пересмотр реализуемых мероприятий в области ИБ.

5. Структура внутренних нормативных документов

5.1. Структура и иерархия ВНД Компании и ее ДО по ИБ представлена на рисунке 2.



Рисунок 2. Структура ВНД Компании

5.2. **Документом первого уровня** является настоящая Политика.

5.3. **Документы второго уровня** – частные политики ИБ, которые детализируют положения настоящей Политики применительно к одному или нескольким процессам ИБ, видам и применяемым технологиям.

5.4. Частные политики ИБ разрабатываются и вводятся в действие по мере развития СОИБ Компании и ее ДО.

5.5. Последовательность и приоритеты разработки и внедрения частных политик по ИБ определяются на основании результатов проведенных аудитов и/или самооценки ИБ.

5.6. **Документы третьего уровня** (положения и регламенты) описывают порядок выполнения действий или операций, связанных с ИБ, устанавливают правила и требования по обеспечению ИБ в рамках конкретных бизнес-процессов Компании и ее ДО.

5.7. **Документы четвертого уровня** – инструкции, приказы, акты, реестры, отчеты, модели угроз и иные низкоуровневые документы по обеспечению ИБ.

6. Ответственность

6.1. Нарушение/невыполнение работниками Компании и ее ДО требований по обеспечению ИБ и своевременному информированию об инцидентах в сфере ИБ приравнивается к неисполнению/ненадлежащему исполнению возложенных на них должностных обязанностей и влечет применение мер дисциплинарного воздействия в установленном порядке.

6.2. В случаях, когда нарушение/невыполнение работниками Компании и ее ДО требований по обеспечению ИБ привело к значительным негативным последствиям и/или материальному ущербу, или существенной угрозе возникновения значительных негативных последствий и/или материального ущерба, в качестве дисциплинарной меры Компанией может быть принято решение о расторжении трудового договора с виновным работником в установленном законодательством порядке.