ГРИНАТОМ
РОСАТОМ

АКЦИОНЕРНОЕ ОБЩЕСТВО «ГРИНАТОМ»
(АО «Гринатом»)

ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ «СИСТЕМА ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ДОСТУПОМ ПОЛЬЗОВАТЕЛЕЙ»

Москва
2024

24.04.2024 22/493-РДП

СОДЕРЖАНИЕ

1. Перечень сокращений, терминов и определений

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

Автоматизированная система в защищенном исполнении (АСЗИ) – автоматизированная система акционерного общества «Гринатом», филиала акционерного общества «Гринатом»**, обособленного подразделения** акционерного общества «Гринатом», **реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или иных нормативных документов по защите информации.**

Автоматизированное рабочее место (АРМ) – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

Администратор информационной безопасности (АИБ) – лицо, уполномоченное выполнять действия по администрированию (управлению) системой защиты информации в соответствии с установленной ролью.

Администратор средства защиты информации (Администратор СрЗИ) – администратор, выполняющий работы по поддержке функционирования средств защиты информации или сертифицированных операционных систем или сертифицированного прикладного программного обеспечения.

Безопасность информации – состояние защищённости информации, при котором обеспечивается её конфиденциальность, доступность и целостность.

Владелец информационного ресурса – лицо (либо структурное подразделение), получившее на законных основаниях право разрешать или ограничивать доступ к информационному ресурсу.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы автоматизированной системы.

Доступ к информации – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная безопасность (ИБ) – сохранение конфиденциальности, целостности и доступности информации.

Информационные ресурсы – используемые в информационных системах Госкорпорации «Росатом», АО «Гринатом» (филиалах и обособленном подразделении АО «Гринатом») документы, файлы и базы данных, распоряжение

доступом, к которым осуществляется их обладателем путем установления соответствующих правил.

Информационные технологии (ИТ) – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения (сообщения, данные), независимо от формы их представления.

Информация ограниченного доступа – информация, доступ к которой ограничен на основании законодательства Российской Федерации, отраслевым нормативным документами Госкорпорации «Росатом» и локальным актам АО «Гринатом».

Инцидент информационной безопасности – одно или несколько нежелательных, или неожиданных событий информационной безопасности, которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для информационной безопасности.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Контроль доступа – проверка выполнения субъектами доступа установленных правил разграничения доступа в автоматизированной системе.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, отраслевыми нормативными документами по Госкорпорации «Росатом» и локальными актами АО «Гринатом».

Корпоративный центр ГосСОПКА (КЦ ГосСОПКА) – центр ГосСОПКА, созданный государственными корпорациями, операторами связи и иными организациями, осуществляющими лицензируемую деятельность в области защиты информации, в собственных интересах, а также для оказания услуг по предупреждению, обнаружению и ликвидации последствий компьютерных атак.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Персональные данные (ПДн) – любая информация, относящаяся к прямо либо косвенно определенному или определяемому физическому лицу.

Работники – физические лица, выполняющие трудовые обязанности на основании заключенных трудовых и гражданско-правовых договоров.

Сотрудники – физические лица, выполняющие обязанности согласно должностной инструкции на основании заключенных гражданско-правовых договоров.

Служебная информация ограниченного распространения - несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой, диктуются служебной необходимостью.

Событие безопасности – выявленное состояние системы, услуги или состояния сети, указывающее на возможное нарушение политики обеспечения информационной безопасности, нарушение или отказ мер и средств контроля и управления или прежде неизвестная ситуация, которая может иметь значение для безопасности.

Средство защиты информации (СрЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Целостность – свойство сохранения правильности и полноты информации.

DRP – план аварийного восстановления.

2. Общие положения

Настоящий документ разработан в целях реализации организационных мер по защите информации, обрабатываемой в информационной системе «Система централизованного управления доступом пользователей» (далее – СЦУДП).

Инструкция администратора информационной безопасности СЦУДП (далее – Инструкция) определяет порядок действий администратора информационной безопасности (далее – администратор ИБ), направленных на обеспечение безопасности информации, обрабатываемой в СЦУДП.

К информации ограниченного доступа, обрабатываемой в СЦУДП, относится информация, не содержащая сведений, составляющих государственную тайну (далее – конфиденциальная информация):

служебная информация ограниченного распространения (с ограничительной пометкой «Для служебного пользования»)[1];

персональные данные.

Данный документ описывает функции и порядок работы администратора ИБ СЦУДП.

В соответствии с категориями АИБ[2], определенными в АО «Гринатом» АИБ СЦУДП относится к категории: администраторы, выполняющие работы по поддержке функционирования сертифицированного в системе сертификации ФСТЭК России прикладного программного обеспечения.

Целью разработки настоящей Инструкции является определение:

основных задач и функций АИБ СЦУДП;

прав АИБ СЦУДП;

ответственности, возлагаемой на АИБ СЦУДП;

---

1 Перечень сведений, составляющих служебную информацию ограниченного распространения («Для служебного пользования»).

2 Положение о порядке организации и проведении работ по защите информации ограниченного доступа АО Гринатом

порядка обучения и информирования пользователей об угрозах безопасности информации и правилах эксплуатации АСЗИ и отдельных СрЗИ;

порядка эксплуатации СрЗИ;

порядка внесения изменений в технический паспорт и перечень защищаемых ресурсов;

порядка внесения изменений в правила разграничения доступа, регламентирующих права доступа пользователей к объектам доступа, и введения ограничений на их действия;

порядка хранения и использования средств восстановления СрЗИ;

порядка изменения условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

порядка контроля целостности системных ресурсов;

порядка периодического контроля СрЗИ;

порядка осуществления контроля за событиями безопасности и действиями пользователей в СЦУДП.

В своей деятельности АИБ СЦУДП должен руководствоваться:

нормативными правовыми актами, методическими документами и национальными стандартами Российской Федерации в области защиты информации;

распорядительными документами Госкорпорации «Росатом», приказами, распоряжениями и указаниями вышестоящего руководства;

внутренними нормативными документами Госкорпорации «Росатом»;

настоящей и должностной инструкциями.

АИБ СЦУДП должен обладать следующими знаниями:

законодательство Российской Федерации в области защиты информации;

отраслевая и корпоративная нормативно-методическая документация;

средства защиты информации, используемые в СЦУДП;

порядок взаимодействия со смежными подразделениями, обеспечивающими безопасное функционирование СЦУДП и предоставляющими услуги в части ИБ.

АИБ СЦУДП должен обладать следующими навыками:

экспертиза и актуализация, в части обеспечения безопасности информации, документации на СЦУДП;

проведение внутренних аудитов ИБ;

уверенная работа со специализированным программным обеспечением и офисным программным обеспечением;

администрирование СрЗИ, используемых в СЦУДП;

взаимодействие с пользователями СЦУДП и подразделениями, предоставляющими услуги в части ИБ.

АИБ СЦУДП должен руководствоваться в своей деятельности:

нормативными правовыми актами, методическими документами и национальными стандартами Российской Федерации в области защиты информации;

локально-нормативными актами, распорядительными документами, приказами, распоряжениями Госкорпорации «Росатом» и указаниями вышестоящего руководства;

организационно-распорядительной и эксплуатационной документацией на СЦУДП;

эксплуатационной документацией на сертифицированные средства зашиты информации, входящей в пакет сертификации;

настоящей и должностной инструкциями.

В рамках исполнения п. 4.13 «Повышение осведомленности персонала в области ИБ» приказа Госкорпорации «Росатом» от 10.02.2021 № 1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях», АИБ СЦУДП должен пройти специализированное обучение в ИС «Рекорд-мобайл» по направлениям:

«Администрирование информационной безопасности в автоматизированных системах»;

«Защита информации в автоматизированных системах физической защиты»;

«Обеспечение безопасности объектов критической информационной инфраструктуры»;

«Основы информационной безопасности компьютерных систем, применяемых в организациях атомной отрасли»;

«Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа».

На период длительного отсутствия (отпуска, болезни, командировки) основного АИБ СЦУДП должен назначаться временно исполняющий обязанности АИБ СЦУДП работник, обладающий знаниями и навыками работы администратора ИБ.

АИБ СЦУДП должен быть ознакомлен под подпись с настоящей инструкцией. Лист ознакомления приведён в приложении к настоящей инструкции.

3. Основные задачи и функции администратора безопасности информации

Основными задачами АИБ СЦУДП, выполняющего работы по контролю за соблюдением требований по безопасности информации, обрабатываемой в СЦУДП, являются:

сопровождение сертифицированного в системе сертификации ФСТЭК России прикладного программного обеспечения – программное средство «Система централизованного управления доступом пользователей» (далее – СрЗИ СЦУДП (АРИДА)).

контроль сопровождения администраторами СрЗИ, сертифицированных системных и прикладных программных средств, функционирующих в СЦУДП, на этапе их жизненного цикла и при выводе их из эксплуатации;

контроль за соблюдением администраторами требований по безопасности информации и локальных нормативных актов при эксплуатации СЦУДП;

контроль за работой пользователей СЦУДП и реагирование на инциденты с учётом событий безопасности, регистрируемых применяемыми средствами и механизмами защиты информации;

разработка и внесение предложений по совершенствованию систем и механизмов защиты информации в СЦУДП.

Для выполнения поставленных задач на АИБ СЦУДП возлагаются следующие функции:

администрирование и сопровождение СрЗИ СЦУДП (АРИДА) на этапах его жизненного цикла и при выводе из эксплуатации;

мониторинг событий безопасности, в том числе анализ событий безопасности, регистрируемых средствами и механизмами защиты информации, выявление инцидентов ИБ, реагирование на инциденты ИБ;

организация и контроль допуска пользователей к ресурсам, обрабатывающим конфиденциальную информацию, включая согласование заявок в СЦУДП на доступ пользователей (присвоение ролей) в СЦУДП;

участие в разработке требований по защите информации в СЦУДП, в том числе участие в экспертизе технических заданий, проектов, решений;

разработка документов (анализ степени конфиденциальности информации, служебная записка для рассмотрения материалов ПДТК, разрешение на информационный обмен), требуемых для реализации интеграции ИС с СЦУДП;

участие в создании и контроле исполнения администраторами требований по защите информации в СЦУДП, в том числе требований организационно-распорядительной документации;

организация и контроль допуска администраторов и пользователей к работе с конфиденциальной информацией;

предотвращение возможности нарушений требований информационной безопасности;

участие в анализе материалов событий безопасности СЦУДП, выявление инцидентов ИБ, реагирование на инциденты ИБ;

реагирование на события безопасности в части выявления и расследования причин возникновения событий безопасности с привлечением, при необходимости, администраторов и ответственных должностных лиц в части устранения последствий инцидентов ИБ, а также, предотвращения аналогичных инцидентов ИБ в будущем;

организация и контроль проведения мероприятий аудита за соответствием состояния СрЗИ установленным требованиям;

выполнение мероприятий по контролю целостности компонент СрЗИ СЦУДП (АРИДА);

проведение мероприятий аудита за соответствием состояния СрЗИ СЦУДП (АРИДА) установленным требованиям;

контроль за наличием уязвимостей, которые могут быть использованы для нанесения компьютерных атак на защищаемые ресурсы СЦУДП, и их ликвидация совместно с администраторами СЦУДП;

взаимодействие с администраторами СрЗИ, в части обновления версий СрЗИ и сертифицированных системных и прикладных программных средств, установленных в ИС СЦУДП;

взаимодействие с администраторами КЦ ГосСОПКА в части проведения мероприятий по оперативному реагированию и ликвидации последствий компьютерных атак и компьютерный инцидентов в информационных ресурсах СЦУДП;

взаимодействие с испытательными лабораториями, ФСТЭК России в части поддержания сертификата соответствия требованиям ИБ СрЗИ СЦУДП (АРИДА);

участие в проводимых на специализированных площадках мероприятиях, посвященных информационной безопасности;

подготовка предложений по развитию и обучению сотрудников, выполняющих функции администраторов.

4. Функциональные и должностные обязанности администратора информационной безопасности

Функциональные обязанности АИБ СЦУДП:

уведомлять непосредственного руководителя о намерении убытия за пределы Российской Федерации;

знание требований Единых отраслевых методических указаний по информационной безопасности; [3]

знание состава, порядка эксплуатации и перечня решаемых задач эксплуатируемых средств и механизмов защиты информации в СЦУДП;

контроль обеспечения бесперебойного функционирования средств и механизмов защиты информации СрЗИ СЦУДП (АРИДА);

ведение учета и управление конфигурациями сопровождаемого СрЗИ СЦУДП (АРИДА) и его механизмов защиты информации согласно действующим политикам;

контроль соответствия технического паспорта и перечня защищаемых ресурсов объектов информатизации, своевременного внесения изменений;

проведение периодического контроля целостности СрЗИ СЦУДП (АРИДА);

проведение периодического выборочного тестирования правильности настройки СрЗИ СЦУДП (АРИДА) и его механизмов защиты информации;

участие в проведении периодического анализа защищенности СЦУДП;

---

[3] Приказ Госкорпорации «Росатом» от 10.02.2021 № 1/140-П-дсп «Об утверждении единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и её организациях».

участие в организации, координации и контроля (мониторинга) выполнения мероприятий по защите информации в СЦУДП;

разработка (согласование) требований по защите информации в СЦУДП, в том числе участие в экспертизе технических заданий, проектов, решений при создании или внедрении изменений в АС (ИС, ОКИИ), участие в определении и анализе достаточности реализованных мер защиты информационных ресурсов и т.п.;

участие в организации (разработке, согласовании) разрешительной системы доступа и контроль доступа работников, сотрудников и сторонних лиц к работе с информацией ограниченного доступа в СЦУДП;

обеспечение доступа пользователей к информационным ресурсам и работе с информацией ограниченного доступа согласно принятой разрешительной системе («Матрице доступа»);

анализ содержимого журналов событий безопасности СрЗИ СЦУДП (АРИДА) и механизмов защиты информации или специального программного обеспечения по регистрации событий безопасности в СЦУДП;

контроль своевременного архивирования журналов событий и обеспечение надлежащего режима их хранения с установленной периодичностью;

хранение средств восстановления СрЗИ СЦУДП (АРИДА) и их периодическое тестирование;

восстановление работоспособности СрЗИ СЦУДП (АРИДА) совместно с администраторами ИС и механизмов защиты информации при выходе их из строя вследствие нештатных (аварийных) ситуаций или устранения последствий стихийного или техногенного характера;

проведение расследований инцидентов информационной безопасности СЦУДП;

проведение и анализ результатов внутренних аудитов информационной безопасности СЦУДП с целью контроля выполнения установленных требований по защите информации, а также определения необходимости проведения корректирующих и предупреждающих мероприятий (действий);

осуществление непосредственного контроля за внесением изменений в конфигурацию (модификацию) программных, программно-аппаратных средств и механизмов защиты информации СЦУДП, установкой и настройкой программного обеспечения для обработки информации ограниченного доступа, средств защиты информации;

участие в разработке, согласовании и внесении изменений в нормативную документацию, регламентирующую правила и требования по безопасности обрабатываемой информации;

ежегодное прохождение курсов обучения по вопросам информационной безопасности в системе развития кадрового потенциала ИС «РЕКОРД»[4];

соблюдение общепринятых правил деловой этики и норм общения, а также рамок законодательства Российской Федерации и отраслевой, нормативной и методической документации Госкорпорации «Росатом» и АО «Гринатом»;

выявление и информирование руководителей, по порядку подчиненности, по выявлению новых угроз безопасности информации и по фактам, имеющим место, попыткам совершения несанкционированных действий;

доведение до непосредственного руководителя информации обо всех выявленных недостатках и несоответствиях в пределах своей компетенции.

В обязанности администратора ИБ также входит:

участие в организации, координации и контроле выполнения мероприятий по защите информации пользователями СЦУДП;

участие в определении требований по защите информации в СЦУДП, участие в определении и анализе достаточности реализованных мер защиты информационных ресурсов в СЦУДП, поддержание в актуальном состоянии реализованных мер в соответствии с требованиями федерального законодательства, регуляторов в области информационной безопасности, включая приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», а также отраслевых и корпоративных нормативных актов;

участие в разработке, согласовании и внесении изменений в нормативную документацию, регламентирующую правила и требования по безопасной работе в СЦУДП, в том числе приказом АО «Гринатом» от 21.05.2020 № 22/454-П «Об утверждении Регламента по согласованию доступа к ресурсам Центра обработки данных Госкорпорации «Росатом» и сетевых взаимодействий между автоматизированными системами в защищенном исполнении и/или информационными системами предприятий отрасли», от 11.05.2022 № 22/286-П-дсп «Об утверждении «Регламента предоставления доступа к системам разработки»;

реагирование на инциденты информационной безопасности в соответствии с приказом АО «Гринатом» от 27.08.2020 № 22/719-П-дсп «Об утверждении порядка взаимодействия отраслевого Корпоративного центра ГосСОПКА Госкорпорации

---

[4] Обязательные курсы обучения:
1. Администрирование информационной безопасности в автоматизированных системах;
2. Обеспечение безопасности объектов критической информационной инфраструктуры;
Дополнительные курсы обучения:
1. Основы информационной безопасности компьютерных систем, применяемых в организациях атомной отрасли;
2. Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа.

«Росатом» с подразделениями АО «Гринатом» в процессе реагирования на инциденты информационной безопасности»;

выполнение рекомендаций Корпоративного центра ГосСОПКА Госкорпорации «Росатом»;

участие в проведении расследований инцидентов ИБ и ликвидации их последствий;

взаимодействие с Корпоративным центром ГосСОПКА Госкорпорации «Росатом» для предотвращения кибератак и ликвидации их последствий;

выполнение положений приказа АО «Гринатом» от 30.11.2022 № 22/573-П «Порядок процесса «Действия в аварийных ситуациях»;

участие в проведении и анализе результатов внутренних аудитов информационной безопасности с целью определения выполнения установленных требований по защите информации в СЦУДП, а также выявления возможных улучшений и определения необходимости проведения корректирующих и предупреждающих мероприятий;

контроль доступа и проверка полномочий пользователей на основании приказа Госкорпорации «Росатом» от 30.12.2019 № 1/1517-П «Об утверждении Единые отраслевые методические указания по предоставлению пользователям доступа к централизованным ИТ-ресурсам Госкорпорации «Росатом» и организаций Госкорпорации «Росатом» и ролевой модели СЦУДП;

мониторинг и анализ работы пользователей;

предотвращение возможности нарушений требований информационной безопасности в СЦУДП, контроль за работой пользователей и администраторов СЦУДП;

осуществление консультаций пользователей СЦУДП по правилам безопасной и корректной работы в СЦУДП;

хранение контрольных копий лицензионного программного обеспечения и СрЗИ, документации на СрЗИ в соответствии с приказом АО «Гринатом» от 04.10.2023 № 22/424-П «Об утверждении и введении в действие Порядка оказания услуг резервного копирования и восстановления информационных систем находящихся на обслуживании АО «Гринатом», контроль соответствия контрольных сумм, установленных программных СрЗИ приведённым в документации;

осуществление непосредственного контроля за внесением изменений в конфигурацию (модификацию) аппаратно-программных средств, используемых в СЦУДП, установку и настройку ПО для обработки информации ограниченного доступа, СрЗИ;

осуществление контроля политик антивирусной защиты и целостности наложенных СрЗИ в соответствии с технологическими инструкциями на систему антивирусной защиты информации, технологическими инструкциями на средства защиты информации и инструкцией по эксплуатации СрЗИ (утверждена приказом АО «Гринатом» от 01.04.2019 № 22/277-П);

отслеживание сроков действия сертификатов соответствия на средства защиты информации, условия функционирования средств защиты информации, своевременное, за 9 месяцев до окончания сроков, уведомление непосредственного руководителя, органа по аттестации, руководителя, ответственного за закупку и поставку необходимых лицензий на средства защиты информации, с целью выявления необходимости и планирования закупки средств защиты информации, проведения оценки соответствия требованиям информационной безопасности;

проведение работ по обновлению средств защиты информации при истечении срока действия сертификатов соответствия, выявления необходимости замены средств защиты информации, устранения уязвимостей;

отслеживание срока действия аттестата соответствия требованиям безопасности информации, выполнение условий эксплуатации и функционирования СЦУДП;

информирование непосредственного руководителя и функционального руководителю по направлению ИБ обо всех выявленных недостатках и несоответствиях в пределах своей компетенции.

5. Права администратора информационной безопасности

Администратор ИБ имеет право:

требовать от пользователей и (или) системных администраторов СЦУДП предоставления информации в пределах своей компетенции;

требовать от пользователей СЦУДП соблюдения установленной технологии обработки информации и выполнения руководств, инструкций и положений по обеспечению защиты информации;

осуществлять контроль за деятельностью пользователей и системных администраторов СЦУДП;

согласовывать самостоятельные решения в области деятельности предусмотренной настоящей Инструкцией;

вносить на рассмотрение непосредственному руководителю предложения по улучшению и усовершенствованию деятельности и существующих технических решений в пределах своей компетенции;

формировать и оформлять материалы, необходимые для проведения внутренних расследований по действию пользователей и системных администраторов СЦУДП;

по согласованию с руководством, принимать участие в мероприятиях, способствующих повышению квалификации по профилю своей деятельности;

непосредственно обращаться к руководителям структурных подразделений с требованием организовать прекращение работы пользователя, нарушившего установленную технологию обработки защищаемой информации;

осуществлять оперативное вмешательство в работу пользователей или СрЗИ при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по

безопасности с последующим докладом своему непосредственному руководителю и администратору информационной безопасности, выполняющему работы по контролю за соблюдением требований по безопасности информации;

требовать от АИБ СрЗИ (помимо СрЗИ СЦУДП (АРИДА)), используемых в СЦУДП предоставления информации в пределах своей компетенции;

взаимодействовать с органами государственной власти, надзорными органами, контрагентами в рамках своей компетенции.

6. Ответственность администратора информационной безопасности

Администратор ИБ СЦУДП несёт предусмотренную законодательством Российской Федерации ответственность за:

сопровождение СрЗИ СЦУДП (АРИДА) в процессе его жизненного цикла;

за нарушение правил эксплуатации средств защиты информации, либо правил доступа к СЦУДП;

ненадлежащее выполнение своих должностных или функциональных обязанностей;

полноту и достоверность данных, предоставляемых в ходе выполнения возложенных на него настоящей Инструкцией обязанностей;

непринятие мер при выявлении нарушений безопасности информации СЦУДП;

качество проводимых работ по обеспечению защиты информации в соответствии с функциональными обязанностями;

разглашение сведений, составляющих информацию ограниченного доступа, в том числе о применяемых системах, методах и способах защиты информации СЦУДП;

разглашение ключевой, аутентификационной и идентификационной информации средств защиты информации, администраторов и пользователей;

за создание, распространение и (или) использование компьютерных программ либо иной информации, заведомо предназначенных для неправомерного воздействия на объекты информатизации Госкорпорации «Росатом», в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в них.

соблюдение требований законодательства Российской Федерации и требований локальных нормативных актов Госкорпорации «Росатом» и нормативной и методической документации АО «Гринатом», эксплуатационной документации на СрЗИ, сертифицированное системное и прикладное программное обеспечение.

Администратору ИБ СЦУДП **запрещается**:

используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим (третьим) лицам с целью ее распространения, модификации, копирования, уничтожения;

нарушать правила хранения ключевой, аутентификационной и идентификационной информации;

использовать ставшие доступные ему, в ходе исполнения обязанностей, идентификационные данные пользователей для маскирования своих действий;

использовать в своих и (или) в чьих-либо личных интересах ИТ-ресурсы и предоставлять такую возможность другим;

передавать третьим лицам информацию ограниченного доступа (данные сетевой связанности, сетевые адреса, имена, пароли, информацию о привилегиях пользователей, настройки конфигураций средств и механизмов защиты информации и т.д.);

самостоятельно отключать средства и механизмы защиты информации, кроме случаев оговоренных настоящей Инструкцией и нормативными документами Госкорпорации «Росатом» и АО «Гринатом», а также при выводе их из эксплуатации;

производить действия, приводящие к нарушению порядка функционирования средств и механизмов защиты информации;

нарушать правила эксплуатации программных, аппаратно-программных средств и механизмов защиты информации.

корректировать, удалять, подменять информацию, содержащую регистрационные данные о событиях безопасности, журналы аудита.

самостоятельно (без согласования с администратором ИБ, выполняющим работы по контролю за соблюдением требований по безопасности информации) вносить изменения в настройки средств защиты информации, сертифицированного системного и прикладного программного обеспечения.

7. Порядок информирования пользователей об угрозах безопасности информации и правилах эксплуатации средств защиты информации

В АО «Гринатом» обучение и информирование пользователей об угрозах безопасности информации, о правилах эксплуатации средств защиты информации осуществляется на следующих этапах взаимоотношений с работниками:

при приеме на работу;

во время действия трудового договора;

при переводе на другую должность.

При приеме сотрудника на работу, с ним проводится вводный инструктаж по соблюдению требований информационной безопасности в форме очного или дистанционного обучения. Сотрудник под роспись ознакомляется с Инструкцией пользователя, содержащей информацию об угрозах безопасности информации и о правилах эксплуатации рабочих мест и отдельных средств защиты информации, установленных на рабочие места.

После заключения трудового договора, до сотрудников под подпись доводятся нормативные и методические документы по ИБ АО «Гринатом», в соответствии с выполняемыми ими должностными обязанностями.

Актуальность Инструкции пользователя проверяется АИБ с периодичностью не реже чем 1 раз в полгода, актуальность нормативно-методических документов по информационной безопасности с периодичностью не реже чем 1 раз в год. Инициатором проверки выступает АИБ, выполняющий работы по контролю за соблюдением требований по безопасности информации.

При изменении состава СрЗИ, правил эксплуатации СрЗИ АИБ согласовывает и вносит соответствующие изменения в Инструкцию пользователя. После утверждения внесённых в Инструкцию пользователя изменений она направляется всем сотрудникам для ознакомления под роспись.

При изменении (возникновении новых) угроз безопасности информации, АИБ обобщает и структурирует материал по угрозам безопасности информации и доводит его до сотрудников АО «Гринатом» посредством корпоративной электронной почты.

В случае обнаружения нарушения сотрудником АО «Гринатом» положений Инструкции пользователя или иных нормативных документов АО «Гринатом», АИБ проводит с данным работником разъяснительную беседу и информирует его непосредственного руководителя о произошедшем нарушении.

Информирование работников о необходимости реализации требований защиты информации должно проводиться на регулярной основе не реже одного раза в год путём:

ознакомления с нормативными материалами, методическими рекомендациями и инструкциями;

периодической оценки готовности работников к действиям по защите информации;

проведения дополнительного обучения работников в соответствии с требованиями к квалификации;

рассылки дополнительных информационных материалов по вопросам защиты информации.

Ответственность за проведение информирования возлагается как на уполномоченных работников АО «Гринатом», так и на АИБ.

Контроль за проведением информирования осуществляется со стороны администраторов, выполняющих работы по контролю за соблюдением требований по безопасности информации, обрабатываемой в СЦУДП.

8. Порядок эксплуатации средств защиты информации

К использованию в СЦУДП допускаются сертифицированные, в системе сертификации ФСТЭК России, по требованиям безопасности информации СрЗИ, системное и прикладное программное обеспечение, отвечающие требованиям стандартизации оснащения, установленными локальными правовыми актами Госкорпорации «Росатом» и АО «Гринатом».

В настоящем разделе приведен общий порядок эксплуатации СрЗИ.

Для настройки и сопровождения конкретного средства или механизма защиты информации, необходимо руководствоваться Инструкцией по эксплуатации средств защиты информации и эксплуатационной документацией. Также, АИБ необходимо руководствоваться в своей деятельности требованиями Положения (руководства) о порядке организации и проведении работ по защите информации ограниченного доступа, где приведены особенности эксплуатации СрЗИ относительно их предназначения и среды функционирования.

8.1. Порядок установки СрЗИ

СрЗИ, по вариантам исполнения представлены программными и программно-аппаратными средствами. Программные СрЗИ подразделяются на средства централизованного управления (серверная часть и клиентская часть), автономные и встроенные в состав сертифицированных, в системе сертификации ФСТЭК России, продуктов (например, сертифицированные операционные системы или СУБД).

Установка программных СрЗИ должна производится из сертифицированных дистрибутивов, поставляемых поставщиками СрЗИ.

Установка серверных компонент и компонент централизованного управления СрЗИ, настройка параметров СрЗИ на рабочих станциях и серверах объектов информатизации осуществляется АИБ в соответствии с эксплуатационной документацией на конкретные СрЗИ, а также требованиями защиты информации (политиками), установленными законодательством Российской Федерации, отраслевыми и нормативными актами Госкорпорации «Росатом» и АО «Гринатом».

Установка в СЦУДП СрЗИ, сертифицированных системных и прикладных программных средств, за исключением СрЗИ СЦУДП (АРИДА), допускается Администратором СрЗИ в рамках услуги поддержки СрЗИ.

Для установки отдельных (специализированных) СрЗИ или сертифицированных системных или прикладных программных продуктов, могут привлекаться Администраторы СрЗИ в рамках услуги поддержки, при этом АИБ СЦУДП совместно с Администратором СрЗИ обязан проверить корректность проведённой установки и настроек СрЗИ. Привлечение сотрудников иных соответствующих подразделений АО «Гринатом», в обязательном порядке, согласовывается с Департаментом контроля информационной безопасности и противодействия угрозам АО «Гринатом».

В ходе своей работы средства и механизмы защиты информации не должны нарушать логику работы остальных используемых функциональных приложений. СрЗИ должно работать в режиме штатного функционирования СЦУДП.

8.2. Порядок эксплуатации СрЗИ

При эксплуатации средств и механизмов защиты информации АИБ СЦУДП необходимо соблюдать следующие положения:

средства и механизмы защиты информации удалённо управляются с рабочего места АИБ;

рабочее место АИБ должно находится в пределах контролируемой зоны АО «Гринатом»;

нагрузка функционала СрЗИ на аппаратные (программные) ресурсы СЦУДП не должна препятствовать режиму штатного функционирования СрЗИ;

все средства и механизмы защиты информации должны функционировать в режиме реального времени на протяжении всего времени эксплуатации информационных (аппаратных) ресурсов СЦУДП;

доступ пользователей к информационным ресурсам и работе с информацией ограниченного доступа организуется согласно принятой для СЦУДП разрешительной системы («Матрице доступа»);

аутентификация пользователя осуществляется с использованием паролей и (или) аппаратных средств или в случае двухфакторной аутентификации - определенной комбинации указанных средств;

для пользователей, обладающих правом удаленного доступа к информационным ресурсам СЦУДП, настраивается двухфакторная аутентификация;

доступ к журналам регистрации событий безопасности (штатного функционирования) СрЗИ СЦУДП (АРИДА) предоставляется только АИБ СЦУДП (АРИДА) и, в режиме чтения, сотруднику Департамента контроля информационной безопасности и противодействия угрозам АО «Гринатом», осуществляющему работы по контролю за соблюдением требований по безопасности информации;

конфигурационные параметры, работы и задачи, выполняемые СрЗИ СЦУДП (АРИДА), должны быть настроены согласно требованиями руководящих документов ФСТЭК России и ФСБ России, применяемых к объектам информатизации установленных категорий, классов, уровней защищенности, а также локальных нормативных актов АО «Гринатом»;

изменения в требования к содержанию конфигураций СрЗИ согласовываются с Департаментом контроля информационной безопасности и противодействия угрозам АО «Гринатом»;

АИБ СЦУДП должна проводится проверка настройки конфигурационных параметров на предмет их неизменности или соответствия политикам и контроль целостности компонент СрЗИ (п.8.3), с периодичностью, определенной в «Положении (руководстве) о порядке организации и проведении работ по защите информации ограниченного доступа»;

АИБ СЦУДП обеспечивает хранение (п.8.4) средств восстановления СрЗИ СЦУДП (АРИДА);

контроль состояния СрЗИ СЦУДП (АРИДА) должен осуществляться АИБ (п.8.5) путем проведения выборочного тестирования компонент СрЗИ СЦУДП (АРИДА);

анализ защищенности СЦУДП проводится (инициируется проведение) АИБ с периодичностью, указанной в «Положении (руководстве) о порядке организации и проведении работ по защите информации ограниченного доступа»;

средствами и механизмами защиты информации должно осуществляться оповещение АИБ при следующих событиях:

а) сбоях функционирования компонент системы;

б) попытках несанкционированной модификации компонент системы;

в) успешном (неуспешном) выполнении задач;

г) обнаружении нарушений, установленных на рабочих станциях и серверах требований безопасности информации;

д) успешном (неуспешном) выполнении обновления в заданный период времени соответствующих модулей СрЗИ.

обновление (при необходимости) компонент СрЗИ и системного и прикладного программного обеспечения должно проводится с периодичностью не реже чем 1 раз в 6 месяцев в автоматическом или ручном режиме, за исключением баз данных решающих правил (не реже чем 1 раз в месяц) и антивирусной защиты (ежедневно);

необходимость обновления устанавливается АИБ путем взаимодействия с поставщиками СрЗИ;

АИБ СЦУДП проводится ежемесячный анализ журналов регистрации событий безопасности и режима работы СрЗИ СЦУДП (АРИДА);

СрЗИ СЦУДП (АРИДА) обеспечивается выдача предупреждения АИБ при заполнении установленной части (процент или фактическое значение) объема памяти для хранения информации о событиях безопасности;

при угрозе переполнения, журналы регистрации событий безопасности архивируются и обеспечивается их хранение в течение периода, установленного согласно «Положения (руководства) о порядке организации и проведении работ по защите информации ограниченного доступа»;

при возникновении события безопасности (инцидента), АИБ СЦУДП, в режиме реального времени, предпринимает все возможные меры для предотвращения последствий, немедленно докладывает по факту своему непосредственному руководителю и сотруднику Департамента контроля информационной безопасности и противодействия угрозам АО «Гринатом», выполняющему работы по контролю за соблюдением требований по безопасности информации;

техническое обслуживание СрЗИ должно проводиться в рамках регламентных работ, установленных для СЦУДП в эксплуатационной документации;

АИБ СЦУДП осуществляется контроль соответствия «Технического паспорта» и «Перечня защищаемых ресурсов» СЦУДП, изменения в указанные документы вносятся АИБ при возникновении необходимости.

8.3. Порядок контроля целостности системных ресурсов

Контроль целостности системных ресурсов СЦУДП с целью обеспечения неизменности программной среды, определяемой предусмотренной технологией обработки информации, и защиты от несанкционированного внесения изменений, обеспечивается сертифицированными механизмами СрЗИ от НСД. При проведении проверки проверяется соответствие контрольных сумм системных файлов и файлов СрЗИ их эталонным значениям.

Настройка процедуры контроля целостности осуществляется Администратором СрЗИ, в рамках услуги поддержки СрЗИ, следующим образом:

на сервере управления СрЗИ от НСД запускается механизм контроля программ и данных в централизованном режиме;

все серверы из состава СЦУДП разбиваются на группы с идентичными операционными системами и установленными СрЗИ;

для каждой группы серверов проводится расчёт эталонных значений контрольных сумм системных ресурсов и ресурсов СрЗИ;

для каждой группы серверов создаётся задача проверки соответствия контрольных сумм системных ресурсов и ресурсов СрЗИ рассчитанным эталонным значениям при загрузке операционной системы и при входе в сеанс пользователя;

в случае внесения изменений (модификация, обновление и т.д.) в используемые операционные системы и состав СрЗИ, вносятся изменения в группы и проводится новый расчёт эталонных значений.

Администратор ИБ настраивает СрЗИ от НСД на отправку отчётов на свой адрес электронной почты, в корпоративной почтовой системе, при возникновении нарушения целостности системных ресурсов или компонент СрЗИ.

При обнаружении несанкционированного изменения целостности системных ресурсов или СрЗИ, АИБ должен выполнить следующие действия в зависимости от типа поврежденного объекта:

установить причину нарушения целостности системных ресурсов или СрЗИ;

попытаться восстановить поврежденный объект, если это не затронет работоспособность объекта информатизации в целом и, если объект не был модифицирован случайным образом доверенным процессом;

удалить/заменить на эталонный повреждённый/изменённый объект;

выполнить повторную проверку соответствия файлов объекта эталону.

8.4. Порядок хранения и использования средств восстановления СрЗИ

Под средствами восстановления СрЗИ в рамках Инструкции понимаются:

программные, программно-аппаратные средства, используемые для восстановления функционирования СрЗИ и (или) сертифицированных системных и прикладных программных средств;

дистрибутивы СрЗИ и (или) сертифицированных системных и прикладных программных средств;

документация, описывающая конфигурацию СрЗИ и (или) сертифицированных системных и прикладных программных средств в бумажном или электронном виде.

Дистрибутивы ПО и конфигурация СрЗИ и (или) сертифицированных системных и прикладных программных средств в электронном виде должны храниться на носителях информации, исключающих возможность их перезаписи (например, на дисках CD-R, DVD-R).

Местом хранения носителей информации в электронном виде и документации на материальных (бумажных) носителях должен быть опечатываемый ящик (сейф), доступ к которому предоставляется только АИБ.

При использовании копий документации, последние должны быть заверены уполномоченными лицами.

Контроль выполнения мер по обеспечению безопасности хранения, а также инвентаризации хранящихся средств восстановления СрЗИ, должен проводиться АИБ, выполняющим работы по контролю за соблюдением требований по безопасности информации с периодичностью не реже одного раза в год.

При обновлении дистрибутивов программных, программно-аппаратных средств, внесении изменений в информацию, хранящуюся в электронном виде или на материальных (бумажных) носителях АИБ соответствующим образом должен внести изменения в хранящиеся экземпляры документации, конфигурации и дистрибутивов ПО.

Средства восстановления СрЗИ применяются АИБ в следующих случаях:

восстановление СрЗИ и (или) сертифицированных системных и прикладных программных средств при нарушении их работоспособности;

в ходе проведения тестирования средств восстановления;

в ходе проверки наличия и целостности средств восстановления.

Тестирование и восстановление СрЗИ и (или) сертифицированных системных и прикладных программных средств производится в соответствии с эксплуатационной документацией на них.

Тестирование работоспособности средств восстановления должно проводиться АИБ с периодичностью не реже одного раза в год.

Внесение изменений в конфигурационную информацию средств восстановления проводится сразу после внесения изменений в порядок эксплуатации действующих средств.

При возникновении аварийных (нештатных) ситуаций для восстановления СрЗИ необходимо руководствоваться принятым DRP планом по действиям в аварийных и нештатных ситуациях.

После восстановления функционала СЦУДП для СрЗИ проводится тестирование с целью проверки соответствия настроек и конфигураций и устранения выявленных нарушений.

8.5. Порядок периодического контроля средств защиты информации

Под периодическим контролем понимается проверка правильности функционирования механизмов СрЗИ на северах СЦУДП и в сертифицированных системных и прикладных программных средствах.

Периодический контроль проводится АИБ не реже одного раза в месяц.

При периодическом контроле АИБ:

проверяет соответствие настройки доменных политик требуемым значениям, приведённым в документации на СрЗИ и нормативно-методической документации ФСТЭК и ФСБ России;

выборочно проверяет применение политик не менее чем на 10% серверов СЦУДП (объекты, подвергаемые проверке, не должны повторяться при ее следующем проведении);

на произвольно выбранном сервере СЦУДП выполняет действия от имени учётных записей пользователя и системного администратора, приводящие к срабатыванию средств или механизмов защиты информации. После этого проверяет соответствующие журналы и выполненные средством защиты информации или реализованные механизмом защиты действия по оповещению АИБ и ликвидации угрозы безопасности информации.

9. Порядок изменения условий эксплуатации, состава и конфигурации технических средств и программного обеспечения

Все изменения условий эксплуатации, состава и конфигурации технических средств и программного обеспечения СЦУДП должны производиться только на основании заявок руководителей структурных подразделений. Заявки согласовываются, установленным порядком, с учётом требований, предъявляемых к аттестованным объектам информатизации. Перед внесением изменений, АИБ должен проверить наличие согласованной заявки.

Право внесения изменений в конфигурацию программных, программно-аппаратных средств предоставляется уполномоченным исполнителям:

в отношении изменения условий эксплуатации, состава и конфигурации технических средств и программного обеспечения - работникам подразделения поддержки пользователей или иных соответствующих подразделений АО «Гринатом»;

в отношении программно-аппаратных СрЗИ, за исключением СрЗИ СЦУДП (АРИДА) – Администраторам СрЗИ в рамках услуги поддержки СрЗИ;

Порядок изменения условий эксплуатации, состава и конфигурации технических средств и программного обеспечения:

начальник структурного подразделения АО «Гринатом» оформляет заявку на внесение изменений;

Департамент контроля информационной безопасности и противодействия угрозам АО «Гринатом» подтверждает производственную необходимость

проведения указанных в заявке изменений и отсутствие нарушений требований безопасности информации;

утверждённая заявка передаётся уполномоченному исполнителю для проведения работ по заявке;

руководитель подразделения допускает уполномоченных исполнителей для непосредственного исполнения работ при предъявлении утверждённой заявки;

если для проведения работ по утверждённой (согласованной) заявке необходимо внесение временных изменений в состав или настройки СрЗИ на серверах СЦУДП, то данные работы проводятся уполномоченными исполнителями под контролем АИБ;

установка и обновление программного обеспечения производится с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком, или с эталонных копий программных средств;

после завершения работ по внесению изменений в состав и конфигурацию технических средств, их системные блоки (корпуса технических средств) должны быть опломбированы (опечатаны);

по завершению выполнения работ по заявке, уполномоченные исполнители делают отметку о выполнении и передают исполненную заявку АИБ;

на основании исполненной заявки АИБ вносит изменения в организационно-распорядительные документы.

10. Порядок внесения изменений в технический паспорт и перечень защищаемых ресурсов

АИБ должен знать состав ОТСС, СрЗИ и сертифицированного системного и прикладного программного обеспечения, внедренного в СЦУДП и находящегося в его зоне ответственности. АИБ постоянно отслеживаются вносимые в СЦУДП изменения.

Информация об изменениях АИБ может поступать как в ходе личного общения, так и через портал СУИТ и электронную почту. Источниками информации для АИБ являются системные администраторы, непосредственное руководство и (или) проектная команда.

При необходимости (в случае отсутствия информации), но не реже чем 1 раз в месяц, АИБ самостоятельно инициирует запрос указанной информации.

Полученная информация обобщается и, при наличии изменений, дублируется на АИБ, выполняющего работы по контролю за соблюдением требований по безопасности информации.

В случае невозможности получения или недостаточной точности полученной информации, АИБ самостоятельно запрашивает у Департамента контроля информационной безопасности и противодействия угрозам АО «Гринатом» проведение инвентаризации СЦУДП.

При наличии изменений АИБ заводит в единую отраслевую систему электронного документооборота (ЕОСДО) акт о произошедших изменениях,

согласует его с ответственными лицами АО «Гринатом» и руководителем Департамента контроля информационной безопасности и противодействия угрозам АО «Гринатом» и (или) лицензиатом по технической защите конфиденциальной информации, выдавшей аттестат соответствия СЦУДП требованиям безопасности информации. Регистрационный номер согласованного акта АИБ вносится в Лист регистрации изменений технического паспорта СЦУДП.

Анализ соответствия действующих защищаемых ресурсов СЦУДП установленному перечню проводится АИБ с периодичностью не реже чем раз в квартал. В случае обнаружения несоответствий, АИБ определяет причину возникновения нового защищаемого ресурса или исключения существовавшего защищаемого ресурса, после чего вносит информацию в акт о произошедших изменениях и уведомляет об этом АИБ, выполняющего работы по контролю за соблюдением требований по безопасности информации и лицензиата по технической защите конфиденциальной информации, выдавшего аттестат соответствия СЦУДП требованиям по безопасности информации.

Порядок согласования для Акта изменений перечня защищаемых ресурсов идентичен согласованию Акта изменений в Технический паспорт.

11. Порядок внесения изменений в правила разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введения ограничений на их действия

Основной задачей АИБ в рамках процедур управления изменениями является предотвращение негативных последствий и минимизация потенциальных рисков информационной безопасности, которые могут возникнуть в процессе или после реализации изменений.

Порядок внесения изменений АИБ в правила разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введения ограничений на их действия включает в себя:

определение предполагаемых к внесению изменений в правила разграничения доступа относительно всех объектов защиты;

проведение планирования процедуры внесения изменений, тестирование внесения изменений и анализ предполагаемого результата;

согласование предлагаемых изменений со своим непосредственным или функциональным руководителем и руководителем Департамента контроля информационной безопасности и противодействия угрозам АО «Гринатом»;

внесение согласованных изменений в правила разграничения доступа;

устранение неисправностей, в случае их возникновения, в процессе проведения изменений;

регистрацию произведенных изменений в правила разграничения доступа в организационно-распорядительной и рабочей документации;

информирование о внесённых изменениях всех заинтересованных лиц.

Приложение

Лист ознакомления

№	ФИО	Должность	Дата	Подпись

Руководитель подразделения _____

Ф.И.О. подпись