Приложение
к приказу НИЦ «Курчатовский институт»
от «03» 07 2025 г. № 2470

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
НИЦ «КУРЧАТОВСКИЙ ИНСТИТУТ»

г. Москва
2025 г.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Безопасность информации	–	состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность (ГОСТ Р 50922-2006)
ДКЦТ	–	Департамент координации цифровой трансформации
Доступность информации	–	состояние информации, при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно (ГОСТ Р 50.1.053-2005)
Защита информации	–	деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (ГОСТ Р 50922-2006)
Защищаемая информация	–	информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922-2006)
Защищаемое помещение	–	специальное помещение, в котором планируется в ходе закрытых переговоров, совещаний, встреч обсуждать информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну
Информационная безопасность (ИБ)	–	сохранение конфиденциальности, целостности и доступности информации (ГОСТ Р ИСО/МЭК 27000-2021)
Информационная инфраструктура	–	информационные ресурсы, а также сети электросвязи, используемые для организации их взаимодействия (ГОСТ Р 59709-2022)
Информационные ресурсы	–	информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления (ГОСТ Р 59709-2022), а также данные и/или документы, организованные для получения информации, представленные в любой знаковой системе, на любом физическом носителе и/или распространяемые в информационно-телекоммуникационных сетях (ГОСТ Р 7.0.107-2022)
Информационный актив	–	различные виды информации, которые имеют ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении, в том числе, циркулирующие в информационной

		системе (служебная, управляющая, аналитическая, деловая и т.д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение)
Информация	–	сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 № 149-ФЗ)
Информационная система	–	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 149-ФЗ)
Инцидент информационной безопасности	–	непредвиденное или нежелательное событие (группа событий) информационной безопасности, которое привело (могут привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации (ГОСТ Р 59709-2022)
Канал связи	–	одновременное соединение между двумя станциями для одного вызова, включая внутристанционные соединительные линии, которыми заканчивается канал связи (ГОСТ Р 59502-2021)
Конфиденциальность информации	–	недоступность для неавторизованных лиц, объектов или процессов (ГОСТ Р ИСО/МЭК 27000-2021)
Организации Центра		филиалы (представительства) Центра и организации (учреждения), в отношении которых Центр осуществляет от имени Российской Федерации полномочия учредителя и собственника имущества
Система защиты информации (СЗИ)		совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (ГОСТ Р 50922-2006)
Событие информационной безопасности	–	зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой средств ЗИ, или ситуацию, которая может быть

значимой для безопасности информации (ГОСТ Р 59709-2022)

Средство защиты информации	–	техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (ГОСТ Р 50922-2006)
Угроза безопасности информации	–	совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (ГОСТ Р 50922-2006)
Уязвимость	–	слабое место актива или меры обеспечения информационной безопасности, которое может быть использовано одной или несколькими угрозами безопасности информации (ГОСТ Р ИСО/МЭК 27000-2021)
Целостность информации	–	состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право (ГОСТ Р 50922-2006)
Центр	–	федеральное государственное бюджетное учреждение «Национальный исследовательский центр «Курчатовский институт»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности (далее – Политика ИБ) определяет основные принципы, направления и требования по защите информации, является основным руководящим документом по вопросам информационной безопасности и основополагающим для разработки других документов в части информационной безопасности.

1.2. Настоящая Политика ИБ разработана в соответствии с законодательными актами и нормативными документами Российской Федерации по обеспечению информационной безопасности и является локальным нормативным документом постоянного действия.

1.3. Положения настоящей Политики уточняются в принимаемых Центром и организациями Центра внутренних нормативных документах по информационной безопасности, такими как приказы, регламенты, положения, требования, инструкции.

1.4. Положения Политики ИБ не распространяются на информацию, содержащую сведения, составляющие государственную тайну.

1.5. Настоящая Политика распространяется на все структурные подразделения Центра и организации Центра и является обязательной для исполнения всеми работниками и третьими лицами, имеющими доступ к защищаемой информации и информационной инфраструктуре Центра и/или организаций Центра.

1.6. Обеспечение информационной безопасности – необходимое и обязательное условие для успешного осуществления уставной деятельности.

2. ЦЕЛИ И ЗАДАЧИ

2.1. Политика ИБ направлена на достижение следующих целей:

- определение единого подхода к обеспечению информационной безопасности;

- создание методологической базы для разработки организационно-распорядительных документов по информационной безопасности;

– обеспечение условий для устойчивого и бесперебойного функционирования информационной инфраструктуры Центра и организаций Центра;

– выполнение требований действующего законодательства Российской Федерации, нормативных документов и методических рекомендаций регуляторов в области ИБ.

2.2. Основными задачами Политики ИБ являются:

– создание механизмов управления централизованной системой защиты цифровой информации;

– обеспечение конфиденциальности, целостности, доступности создаваемой и обрабатываемой информации;

– обеспечение мониторинга событий информационной безопасности и реагирования на инциденты информационной безопасности;

– развитие централизованной системы защиты цифровой информации, совершенствование ее организации, форм, методов и средств предотвращения и нейтрализации угроз безопасности информации, а также минимизации и ликвидации последствий ее нарушения;

– создание системы контроля и процедур по защите информации;

– обеспечение осведомленности работников в области информационной безопасности.

3. ЗАЩИЩАЕМЫЕ ОБЪЕКТЫ

3.1. Объектами, подлежащими защите в целях обеспечения безопасности информационных отношений, являются:

– информация, защита которой предусмотрена нормативными правовыми актами Российской Федерации (далее – информация ограниченного доступа, защищаемая информация);

– информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства её обработки,

передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации;

- информационные активы;
- защищаемые помещения.

4. ПРОЦЕСС ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Обеспечение информационной безопасности должно достигаться за счет комплексного использования совокупности организационно-режимных, технических, программных методов и средств защиты информации, а также осуществления непрерывного, всестороннего контроля эффективности реализованных мер по обеспечению информационной безопасности.

4.2. Выбор конкретных методов и средств защиты информации должен осуществляться на основе правил и требований Политики ИБ, с учетом законодательства и экономической целесообразности.

4.3. Деятельность по обеспечению ИБ должна включать следующие этапы:

- формирование требований к обеспечению информационной безопасности;
- разработка и внедрение системы защиты информации;
- установка и настройка средств защиты информации;
- повышение квалификации или обучение работников, ответственных за администрирование средств защиты информации;
- разработка и утверждение комплекта документации, регламентирующей обработку и обеспечение безопасности информации;
- внедрение организационных мер защиты;
- обучение лиц, использующих средства защиты информации, применяемые в системе защиты информации, правилам работы с ними;
- поддержание осведомленности работников в вопросах информационной безопасности и киберграмотности.

4.4. Обеспечение информационной безопасности должно охватывать следующие процессы:

- организацию (регламентацию) информационной безопасности;
- управление информационными активами;
- контроль доступа к информационным ресурсам;
- обеспечение безопасности коммуникаций (защита каналов связи);
- обеспечение непрерывности функционирования критически важных процессов;
- безопасность при эксплуатации информационных систем;
- контроль изменений в информационных системах и информационных активах;
- регистрацию и мониторинг событий ИБ;
- управление уязвимостями;
- управление инцидентами ИБ;
- повышение осведомленности пользователей в вопросах ИБ.

4.5. Для достижения требуемого уровня ИБ в Центре и организациях Центра должна быть внедрена централизованная система защиты цифровой информации, которая должна включать в себя следующие подсистемы:

- защиты от несанкционированного доступа;
- антивирусной защиты;
- обнаружения вторжений;
- межсетевого экранирования;
- защиты среды виртуализации;
- анализа защищенности;
- криптографической защиты.

Порядок реализации, особенности и требования в отношении каждой из подсистем определяются соответствующими организационно-распорядительными документами.

4.6. Посредством технических средств защиты информации,

применяемых в подсистемах централизованной системы защиты цифровой информации, а также путем применения организационных мер защиты информации в соответствии с нормативными и методическими документами Российской Федерации должны реализовываться базовые меры защиты информации.

4.7. Обязанности по координации работ в рамках обеспечения информационной безопасности Центра возложены на Департамент координации цифровой трансформации, который обеспечивает создание и эксплуатацию централизованной системы защиты цифровой информации. В организациях Центра обязанности по обеспечению информационной безопасности должны быть возложены на соответствующее структурное подразделение.

4.8. Основной целью деятельности подразделения, на которое возложены обязанности по обеспечению информационной безопасности, является поддержание бесперебойного функционирования и соответствия требованиям законодательства Российской Федерации централизованной системы защиты цифровой информации Центра, а также реализация Политики ИБ в соответствии с возложенными задачами. Деятельность подразделения осуществляется совместно с другими структурными подразделениями Центра/организаций Центра.

5. МЕРОПРИЯТИЯ ПО ПОВЫШЕНИЮ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ВОПРОСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. В целях повышения уровня осведомленности в вопросах информационной безопасности и киберграмотности все лица, поступившие на работу, должны пройти первичный инструктаж, предусматривающий ознакомление с базовыми правилами и мерами обеспечения личной и корпоративной информационной безопасности.

5.2. При увольнении работнику необходимо сдать все мобильные технические средства и цифровые активы, предоставленные ему в пользование,

при этом его права доступа к объектам информатизации, в том числе к защищаемым объектам, включая копирование информации, незамедлительно аннулируются.

6. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ

6.1. В целях предотвращения нарушений ИБ должны приниматься исчерпывающие меры по оповещению об инцидентах ИБ. Работники обязаны сообщать в уполномоченное структурное подразделение о любых замеченных или предполагаемых нарушениях безопасности, а также выявленных угрозах безопасности информации.

6.2. Принципы и требования, направленные на профилактику и предотвращение инцидентов ИБ, реагирование на инциденты ИБ, а также ликвидацию их последствий определяются Политикой управления инцидентами ИБ и иными организационно-распорядительными документами.

7. ОТВЕТСТВЕННОСТЬ

7.1. Ответственность за разработку и текущий контроль выполнения требований ИБ в рамках выделенных процессов несет лицо, ответственное за обеспечение информационной безопасности.

7.2. Каждый работник за несоблюдение требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

7.3. Руководство Центра/организаций Цента должно требовать от всех работников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными политиками и процедурами. Уполномоченные работники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- выполнения действующих инструкций по вопросам ИБ;
- данных, находящихся на носителях информации;

- порядка использования работниками информационных ресурсов;

- содержания служебной переписки.

7.4. На руководителей организаций Центра возлагается ответственность за организацию повседневной деятельности и выделение необходимых ресурсов для обеспечения информационной безопасности как неотъемлемой составляющей коммерческих и производственных процессов; за своевременную идентификацию значимых ИТ-активов, назначение ответственных за ИТ-активы и управление доступа к ним; за предъявление установленных требований информационной безопасности к работникам Центра и третьим лицам, использующим ИТ-активы Центра, и контроль за их выполнением.

7.5. На работников организаций Центра возлагается ответственность за соблюдение норм и правил информационной безопасности в своей повседневной служебной (трудовой) деятельности.

7.6. Работники, имеющие доступ к защищаемой информации, несут ответственность в соответствии с действующим законодательством Российской Федерации за ее разглашение, утрату или искажение, а также за нарушение установленного порядка обеспечения ИБ.

8. ПОРЯДОК ПЕРЕСМОТРА

8.1. Политика пересматривается в случае изменения законодательства в сфере ИБ или в случае служебной необходимости.

8.2. При осуществлении процедуры пересмотра Политики учитываются:

– результаты контроля состояния ИБ и предложения структурного подразделения, ответственного за ИБ, о совершенствовании процедур обеспечения ИБ;

– изменения в организационно-штатной структуре Центра;

– изменения в законодательной и нормативной базе по ИБ, произошедшие с момента утверждения предыдущей версии Политики ИБ;

– результаты анализа произошедших инцидентов ИБ, а также уязвимости и угрозы безопасности информации, выявленные в объектах информатизации

Центра за время, прошедшее с момента утверждения предыдущей Политики.

8.3. Процедура пересмотра Политики включает:

– анализ и выявление несоответствий действующей Политики ИБ текущим условиям;

– разработка предложений по совершенствованию Политики ИБ;

– утверждение новой редакции Политики ИБ.