ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
УЧРЕЖДЕНИЕ НАУКИ

ИНСТИТУТ

МОЛЕКУЛЯРНОЙ И КЛЕТОЧНОЙ БИОЛОГИИ

СИБИРСКОГО ОТДЕЛЕНИЯ РОССИЙСКОЙ АКАДЕМИИ НАУК

П Р И К А З

12 мая 2025 г. № 25

г. Новосибирск

Об ответственном за обеспечение
информационной безопасности

В целях выполнения требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

П Р И К А З Ы В А Ю

1. Назначить заместителя директора по общим вопросам Зыкова Ивана Анатольевича ответственным за:

- обеспечение информационной безопасности в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук;

-обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

2. Утвердить прилагаемое Положение о заместителе директора, ответственном за обеспечение информационной безопасности в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук. (Приложение № 1).

3. Разместить Положение о заместителе директора, ответственном за обеспечение информационной безопасности в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук на сайте института.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор, д.б.н. С.А. Демаков

Приложение № 1
к приказу от 12.05.2025 № 25

УТВЕРЖДЕНО
приказом директора ИМКБ СО РАН
от 12.05.2025 № 25

Директор _____ С.А. Демаков

ПОЛОЖЕНИЕ
о заместителе директора, ответственном за обеспечение информационной безопасности в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук

Новосибирск – 2025

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о заместителе директора, ответственном за обеспечение информационной безопасности в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук (далее - Ответственное лицо) определяет полномочия, права, обязанности и ответственность Ответственного лица в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук (далее - Институт), на которого возложена ответственность за:

- обеспечение информационной безопасности Института;
- обеспечение безопасности критической информационной инфраструктуры Института;
- обеспечение безопасности значимых объектов критической информационной инфраструктуры Института (создание систем безопасности и контроль за их функционированием);
- обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

1.2. Ответственное лицо назначается Директором Института из числа его заместителей.

1.3. Ответственное лицо подчиняется непосредственно Директору Института.

1.4. Указания и поручения Ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми работниками Института.

2. КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ

2.1. Ответственное лицо должно назначается из числа заместителей Директора Института, имеющих высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Допускается назначение Ответственным лицом заместителя Директора Института, имеющего высшее образование, с обязательным последующим прохождением назначенным лицом обучения по программе профессиональной переподготовки по направлению «Информационная безопасность».

2.2. Ответственное лицо должно обладать следующими знаниями, умениями, профессиональными компетенциями:

2.2.1 Основные (в том числе производственные, бизнес и управленческие) процессы Института и специфика обеспечения безопасности Института.

2.2.2 Влияние информационных технологий на деятельность Института, в том числе:

- роль и место информационных технологий (в том числе степень интеграции информационных технологий) в процессах функционирования Института;
- зависимость основных процессов функционирования Института.

2.2.3 Информационно-телекоммуникационные технологии, в том числе:
- современные информационно-телекоммуникационные технологии, используемые в Институте;
- способы построения информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления формирования информационных ресурсов (далее - системы и сети), в том числе ограниченного доступа:
- типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами:
- принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей.

2.2.4 Обеспечение информационной безопасности, в том числе:
- цели, задачи, основы организации, ключевые элементы, основные способы и средства обеспечения информационной безопасности;
- цели обеспечения информационной безопасности применительно к основным процессам функционирования Института, реализация и контроль их достижения;
- принципы и направления стратегического развития информационной безопасности в Институте;
- правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Институте, состав и содержание таких документов;
- порядок организации работ по обеспечению информационной безопасности в Институте;
- основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности Института для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности Института;
- основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз;
- возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;
- способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;

- порядок организации взаимодействия структурных подразделений Института при решении вопросов обеспечения информационной безопасности;
- управление проектами по информационной безопасности;
- антикризисное управление и принятие управленческих решений при реагировании на кризисы и компьютерные инциденты;
- планирование деятельности по обеспечению информационной безопасности в Институте;
- формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности Института;
- организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности в Институте;
- внедрение политики;
- организация контроля и анализа применения политики;
- организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности в Институте;
- поддержка и совершенствование деятельности по обеспечению информационной безопасности в Институте;
- организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в Институте;
- организация внедрения способов и средств для обеспечения информационной безопасности в Институте;
- организация мероприятий по анализу и контролю состояния информационной безопасности Института и модернизации (трансформации) процессов функционирования Института в целях обеспечения информационной безопасности в Институте;
- обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;
- организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Института и реагированию на компьютерные инциденты;
- организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в Институте.

2.3. С учетом области и вида деятельности Института от Ответственного лица требуется знание нормативных правовых актов Российской Федерации, методических документов, международных и национальных стандартов в области:

- защиты государственной тайны;
- защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных:

- обеспечения безопасности критической информационной инфраструктуры Российской Федерации:
- обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты:
- создания и обеспечения безопасного функционирования государственных информационных систем и информационных систем в защищенном исполнении:
- создания, обеспечения технических условий установки и эксплуатации средств защиты информации:
- иных нормативных правовых актов и стандартов в области информационной безопасности.

3. ТРУДОВЫЕ (ДОЛЖНОСТНЫЕ) ОБЯЗАННОСТИ

3.1. Ответственное лицо принимает участие в формировании политики Института, отвечает за согласование стратегии развития Института в части вопросов обеспечения информационной безопасности.

3.2. Ответственное лицо:

3.2.1 Организует разработку политики, направленной в том числе на обеспечение и поддержание стабильной деятельности Института и его процессов функционирования в случае проведения компьютерных атак, отвечает за согласование и утверждение политики в Институте, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;

3.2.2 Организует работу по обеспечению информационной безопасности Института, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, формулированию перечня негативных последствий, проведению мероприятий по их недопущению, отслеживанию и контролю эффективности (результативности) таких мероприятий, а также по необходимому информационному обмену;

3.2.3 Организует реализацию и контроль проведения в Институте организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю с учетом меняющихся угроз в информационной сфере, а также самостоятельно Ответственным лицом в результате своей деятельности;

3.2.4 Организует беспрепятственный доступ (в том числе удаленный) должностным лицам Федеральной службы безопасности Российской Федерации и ее территориальных органов к информационным ресурсам, принадлежащим Институту либо используемым Институтом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет», в целях осуществления мониторинга их защищенности, а также работникам структурного

подразделения, осуществляющего функции по обеспечению информационной безопасности;

3.2.5 Организует взаимодействие с должностными лицами Федеральной службы безопасности Российской Федерации и ее территориальных органов, в том числе контроль исполнения указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами по результатам мониторинга защищенности информационных ресурсов, принадлежащих Институту либо используемых Институтом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

3.2.6 Организует контроль за выполнением требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся защиты информации;

3.2.7 Организует развитие информационной безопасности, формирование и развитие навыков работников Института в сфере информационной безопасности;

3.2.8 Организует разработку и реализацию мероприятий по обеспечению информационной безопасности в Институте в соответствии с требованиями по обеспечению информационной безопасности, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации;

3.2.9 Организует контроль пользователей информационных ресурсов Института в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации;

3.2.10 Организует планирование мероприятий по обеспечению информационной безопасности в Институте;

3.2.11 Организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Институте, осуществляет согласование иных документов Института в части обеспечения информационной безопасности;

3.2.12 Организует проведение контроля за состоянием обеспечения информационной безопасности в Институте, включая оценку защищенности систем и сетей, оператором которых является Институт.

3.3. Ответственное лицо:

3.3.1 Осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в Институте, а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в Институте, в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак;

3.3.2 Осуществляет регулярное и своевременное информирование руководства Института о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности в Институте и результатах практических учений по противодействию компьютерным атакам;

3.3.3 Осуществляет контроль за ведением организационно-распорядительной документации, статистического учета и отчетности по курируемым разделам работы;

3.3.4 Осуществляет согласование требований к системам и сетям, оператором которых является Институт, в части обеспечения информационной безопасности;

3.4. Ответственное лицо:

3.4.1 Организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности Института и контролирует их результаты:

3.4.2 Организует и контролирует функционирование системы обеспечения информационной безопасности в Институте;

3.4.3 Координирует деятельность иных структурных подразделений Института по вопросам обеспечения информационной безопасности.

3.5. Ответственное лицо согласовывает политику, технические задания и иную основополагающую документацию в сфере информационных технологий, цифровизации и цифровой трансформации Института

3.6. Ответственное лицо с использованием нормативных правовых документов и методических материалов Федеральной службы безопасности Российской Федерации организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты с информационными ресурсами Института, а также взаимодействие с Национальным координационным центром по компьютерным инцидентам следующим способом:

силами организаций, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3.7. Ответственное лицо обеспечивает планирование и реализацию мероприятий по переводу систем и сетей на отечественные средства защиты информации, а также контроль за соблюдением запрета на использование средств защиты информации, странами происхождения которых являются иностранные государства в соответствии с пунктом 6 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

3.8. Ответственное лицо сопровождает мероприятия по разработке (модернизации) систем и сетей в части информационной безопасности, а также требований нормативных правовых актов, нормативно-технических и методических документов по защите информации и выполнения этих требований.

3.9. Ответственное лицо проводит работу по унификации способов и средств по обеспечению информационной безопасности, иных технических решений в Институте.

3.10. Ответственное лицо принимает меры по совершенствованию обеспечения информационной безопасности в Институте.

3.11. Ответственное лицо повышает на постоянной основе профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности.

3.12. Ответственное лицо выполняет иные обязанности, исходя из возложенной ответственности и поставленных руководством Института задач в рамках обеспечения информационной безопасности Института.

3.13. Ответственное лицо:

3.13.1 Соблюдает и обеспечивает выполнение законодательства Российской Федерации:

3.13.2 В случаях, установленных законодательством Российской Федерации, согласовывает политику с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю;

3.13.3 Представляет по запросам Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю достоверные сведения о результатах реализации политики (фактически достигнутом эффекте и результате) и текущем уровне (состоянии) информационной безопасности в Институте;

3.13.4 Поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности, необходимые для обеспечения информационной безопасности в Институте;

3.13.5 Организовывает при необходимости проведение и участвует в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

3.13.6 Участвует в пределах компетенции в осуществлении закупок товаров, работ, услуг для обеспечения нужд в сфере информационной безопасности.

4. ПРАВА ОТВЕТСТВЕННОГО ЛИЦА

4.1. Ответственное лицо имеет право:

4.1.1 Давать указания и поручения работникам Института в части обеспечения информационной безопасности;

4.1.2 Запрашивать у работников Института информацию и материалы, необходимые для реализации возложенных на Ответственное лицо прав и обязанностей;

4.1.3 Участвовать в заседаниях (совещаниях) коллегиальных органов Института, принятии решений по вопросам деятельности Института, а также по внесению предложений по совершенствованию деятельности Института;

4.1.4 Участвовать в разработке политики, выносить политику на обсуждение, утверждение коллегиальному органу Института;

4.1.5 Представлять результаты реализации политики коллегиальному органу Института;

4.1.6 Принимать решения по вопросам обеспечения информационной безопасности Института;

4.1.7 Взаимодействовать с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и иными федеральными органами исполнительной власти по вопросам обеспечения информационной безопасности, в том числе по вопросам совершенствования законодательства Российской Федерации в области обеспечения информационной безопасности;

4.1.8 Вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности;

4.1.9 Инициировать проверки уровня (состояния) обеспечения информационной безопасности в Институте;

4.1.10 Организовывать на объектах Института мероприятия по информационной безопасности, разрабатывать и представлять Директору Института предложения по внесению изменений в процессы функционирования, принимать другие меры, направленные на недопущение реализации негативных последствий;

4.1.11 Получать доступ в установленном порядке в связи с исполнением своих обязанностей в государственные органы, органы местного самоуправления, общественные объединения и другие организации;

4.1.12 Обеспечивать надлежащие организационно-технические условия, необходимые для исполнения обязанностей Ответственного лица.

5. ОТВЕТСТВЕННОСТЬ ОТВЕТСТВЕННОГО ЛИЦА

5.1. Ответственное лицо в соответствии с законодательством Российской Федерации несет ответственность за;

5.1.1 Неисполнение или ненадлежащее исполнение своих обязанностей;

5.1.2 Действия (бездействие), ведущие к нарушению прав и законных интересов Института;

5.1.3 Разглашение государственной тайны и иных сведений, ставших ему известными в связи с исполнением своих обязанностей;

5.1.4 Достижение целей обеспечения информационной безопасности;

5.1.5 Поддержание и непрерывное развитие информационной безопасности Института для исключения (невозможности реализации) негативных последствий;

5.1.6 Организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности Института;

5.1.7 Нарушения требований по обеспечению информационной безопасности;

5.1.8 Нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.