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. № 26

г. Новосибирск

О мероприятиях по повышению
защищенности информационной
инфраструктуры института

В целях выполнения требований письма Министерства науки и высшего образования Российской Федерации от 27.03.2025 № МН-19/353 «О мерах по повышению защищенности информационной инфраструктуры Российской Федерации»

П Р И К А З Ы В А Ю

1. Утвердить Положение о порядке реагирования на компьютерные инциденты в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук (Приложение № 1).
2. Разместить Положение о порядке реагирования на компьютерные инциденты в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук на сайте Института.
3. Утвердить план мероприятий по повышению защищенности информационной инфраструктуры института (Приложение №2).
4. Утвердить состав Группы реагирования на компьютерные инциденты:
- Зыков И.А. – заместитель директора по общим вопросам (ответственный за обеспечение информационной безопасности);
- Пыкин А.П. – программист;
- Мелешенко С.А. - ведущий программист.
5. Программистам Пыкину А.П., Мелешенко С.А. осуществить проведение мероприятий по повышению защищенности информационной инфраструктуры института (Приложение №2) в срок до 31.12.2025г.
6. Контроль за исполнением приказа оставляю за собой.

Директор, д.б.н. С.А. Демаков

Приложение № 1
к приказу от 12.05.2025 № 26

УТВЕРЖДЕНО
приказом директора ИМКБ СО РАН
от 12.05.2025 № 26

Директор _____ С.А. Демаков

ПОЛОЖЕНИЕ

о порядке реагирования на компьютерные инциденты в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук

1. Общие положения

1.1. Настоящее Положение определяет порядок выявления, классификации, реагирования и ликвидации последствий компьютерных инцидентов в Федеральном государственном бюджетном учреждении науки Институте молекулярной и клеточной биологии Сибирского отделения Российской академии наук (далее - ИМКБ).

1.2. Действие Положения распространяется на все информационные системы, сети, оборудование и пользователей ИМКБ.

1.3. К компьютерным инцидентам (КИ) относятся:

1.3.1 Кибератаки (вредоносное ПО, фишинг, DDoS и др.)

1.3.2 Несанкционированный доступ к данным

1.3.3 Нарушение работы инфраструктуры

1.3.4 Иные события, угрожающие информационной безопасности.

2. Группа реагирования на компьютерные инциденты (ГРКИ):

2.1. Ответственный за обеспечение информационной безопасности (ИБ) – координирует мероприятия по реагированию.

2.2. Программист – осуществляет технический анализ и устранение инцидентов.

3. Порядок реагирования

3.1. Выявление и регистрация

3.1.1 Любой работник при обнаружении инцидента обязан сообщить в ГРКИ.

3.1.2 ГРКИ регистрирует инцидент в журнале учета (форма прилагается).

3.2. Классификация инцидента.

Инциденты делятся на:

3.2.1 Низкий риск – незначительные сбои, не влияющие на работу института.

3.2.2 Средний риск – частичное нарушение работы систем, утечка персональных данных.

3.2.3 Высокий риск – масштабная атака, угроза критической инфраструктуре.

3.3. Действия по устранению

3.3.1 Низкий риск: ГРКИ устраняет собственными силами.

3.3.2 Средний риск: привлекается ответственный за ИБ, составляется план ликвидации.

3.3.3 Высокий риск: созывается группа реагирования, при необходимости – уведомляются внешние агенты.

3.4. Расследование и отчетность

3.4.1 ГРКИ проводит внутреннее расследование по причинам КИ.

3.4.2 По итогам составляется отчет для руководства ИМКБ.

3.5. Восстановление и профилактика

3.5.1 ГРКИ восстанавливает работоспособность систем.

3.5.2 Разрабатываются меры по предотвращению повторных инцидентов.

4. Заключительные положения

4.1 Положение пересматривается ежегодно.

4.2 Изменения утверждаются приказом директора.

Приложения:

1. Форма журнала учета инцидентов.

Приложение № 1
к Положению о порядке реагирования на
компьютерные инциденты
в Федеральном государственном бюджетном
учреждении науки Институте молекулярной и
клеточной биологии Сибирского отделения
Российской академии наук

Форма журнала учета инцидентов

Утверждено:

Ответственный за информационную безопасность ИМКБ СО РАН

_____ /Ф.И.О./

"__" _____ _____ г.

Журнал учета инцидентов

№ п/п	Дата и время обнаружения	Описание инцидента	Классификация (низкий/средний/высокий)	Источник/причина	Ответственный за реагирование	Принятые меры	Дата устранения	Подпись ответственного

Пояснения к заполнению:

1. № п/п – порядковый номер инцидента.
2. Дата и время обнаружения – точные момент выявления.
3. Описание инцидента – краткая суть (атака, сбой, утечка и т.д.).
4. Классификация – уровень риска на момент обнаружения.
5. Источник/причина – предварительный анализ (вредоносный код, ошибка персонала, тех. сбой).
6. Ответственный – ФИО и должность сотрудника, назначенного для реагирования.
7. Принятые меры – действия по устранению (блокировка, обновление, расследование).
8. Дата устранения – момент завершения работ.
9. Подпись – подтверждение закрытия инцидента.

Важно:

- Журнал ведется в электронном виде (например, Excel или специализированная система мониторинга) с ограниченным доступом.
- Для инцидентов высокого риска прилагается отдельный отчет с детальным анализом.
- Хранение: не менее 3 лет (требование 152-ФЗ для персональных данных).