АДМИНИСТРАЦИЯ КЫРИНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА
ЗАБАЙКАЛЬСКОГО КРАЯ
ПОСТАНОВЛЕНИЕ

от 22 июня 2026 года № 473

с. Кыра

Об утверждении Порядка реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения в администрации Кыринского муниципального округа

В целях совершенствования системы защиты информации в администрации Кыринского муниципального округа (далее - администрация), обеспечения информационной безопасности и организации порядка реагирования на события информационной безопасности, руководствуясь ст. 26 Устава Кыринского муниципального округа администрация Кыринского муниципального округа постановляет:

1. Утвердить прилагаемый Порядок реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения в администрации Кыринского муниципального округа.
2. Настоящее постановление, опубликовать в сетевом издании «Ононская правда» https: //ононская правда.рф//, на официальном сайте Кыринского муниципального округа в информационно-телекоммуникационной сети «Интернет».
3. Контроль за исполнением настоящего постановления возложить на Куприянова А.М. – первого заместителя Главы Кыринского муниципального округа.

И. о. главы Кыринского
муниципального округа А.М. Куприянов

УТВЕРЖДЕН
Постановлением администрация
Кыринского муниципального округа
от «22» июня 2026 г. №473

Порядок реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения в администрации Кыринского муниципального округа

I. Общие положения

1. Настоящий Порядок реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения в администрации Кыринского муниципального округа (далее - Порядок) устанавливает действия при возникновении угроз информационной безопасности, обусловленных возможностью несанкционированного доступа к муниципальным информационным ресурсам сторонних лиц (третьих лиц), внедрения и распространения вредоносного программного обеспечения, проведения массированных атак типа «отказ в обслуживании», а также возможными техническими сбоями в работе.

Порядок разработан для администрации Кыринского муниципального округа и подведомственных организаций.

2. В настоящем Порядке используются следующие понятия:

инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность информационных систем или информационную безопасность;

информационное взаимодействие - процесс взаимодействия двух и более участников, целью которого является обработка информации в общих информационных системах и сетях;

участники информационного взаимодействия - пользователи информационных систем (далее - пользователи) администрации Кыринского муниципального округа, системные администраторы, специалисты по информационной безопасности (далее - администраторы безопасности) администрации Кыринского муниципального округа.

3. Действие положений настоящего Порядка распространяется на деятельность администрации Кыринского муниципального округа и подведомственные организации и обязательны к соблюдению всеми сотрудниками администрации Кыринского муниципального округа, участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

4. Задачами настоящего Порядка являются:

организация деятельности сотрудников администрации Кыринского муниципального округа осуществляющих администрирование информационных систем в администрации Кыринского муниципального округа;

определение порядка работы пользователей, системных администраторов и администраторов безопасности;

обеспечение целостности, конфиденциальности и доступности информации;

соблюдение требований правовых актов в области защиты информации.

II. Источники и виды инцидентов информационной безопасности

5. Источниками информации об инцидентах информационной безопасности в администрации Кыринского муниципального округа являются:

факты, выявленные сотрудниками администрации Кыринского муниципального округа

результаты работы средств мониторинга информационной безопасности, аудита (внутреннего или внешнего);

журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;

обращения субъектов персональных данных с указанием инцидента информационной безопасности;

сообщения Министерства жилищно-коммунального хозяйства, энергетики, цифровизации и связи Забайкальского края;

сообщения Федеральной службы технического и экспортного контроля России;

сообщения Федеральной службы безопасности Российской Федерации;

сообщения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций;

иные источники информации.

6. Основными видами инцидентов информационной безопасности в администрации Кыринского муниципального округа являются:

несанкционированный доступ к информационным ресурсам администрации Кыринского муниципального округа;

превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников администрации Кыринского муниципального округа

компрометация учетных записей или паролей;

вирусная атака или вирусное заражение;

сетевые атаки (отказ в обслуживании (DoS-атаки), атаки типа Man-in- the-Middle, сниффер пакетов, переадресация портов, IP-спуфинг, атаки на уровне приложений и другое.

III. Анализ исходной информации

7. При получении информации о несанкционированном воздействии на информационную систему и сеть системный администратор совместно с администратором безопасности обязаны убедиться, что инцидент информационной безопасности не является результатом их собственной ошибки или санкционированных действий.

8. При выявлении инцидента информационной безопасности в администрации Кыринского муниципального округа системному администратору совместно с администратором безопасности необходимо:

принять меры по пресечению несанкционированного воздействия в случае, если на момент выявления оно не завершено;

принять меры по устранению причин возникновения инцидента информационной безопасности;

сохранить образ или содержание информационной системы, в том числе журналы событий (информационного ресурса) на момент обнаружения события (несанкционированного воздействия);

провести мероприятия по восстановлению работоспособности информационной системы (информационного ресурса);

провести служебную проверку с целью выявления причин, которые могли привести к произошедшему несанкционированному воздействию.

9. Администратору безопасности информационной системы, подвергшейся несанкционированному воздействию, необходимо в течение трех рабочих дней с момента обнаружения несанкционированного воздействия представить в Министерство жилищно-коммунального хозяйства, энергетики, цифровизации и связи Забайкальского края результаты служебной проверки и информацию о последствиях несанкционированного воздействия и принятых мерах по устранению причин несанкционированного воздействия.

10. Совместно с результатами служебной проверки администратор безопасности также должен представить в Министерство жилищно-коммунального хозяйства, энергетики, цифровизации и связи Забайкальского края:

наименование информационной системы (информационного ресурса), на которую произведено несанкционированное воздействие;

время несанкционированного воздействия и (или) время обнаружения несанкционированного воздействия;

место несанкционированного воздействия (площадка, на которой размещается информационный ресурс, хостинг);

краткое изложение (описание) произошедшего несанкционированного воздействия и его последствий;

контактные данные (фамилия, имя, отчество, номер телефона, адрес электронной почты) системного администратора или администратора безопасности, ответственного за обеспечение работоспособности информационной системы (информационного ресурса);

правовой акт о создании и (или) вводе в эксплуатацию информационной системы (информационного ресурса);

паспорт информационной системы (при наличии);

договор об обслуживании или о техническом сопровождении (при наличии);

договор об оказании услуг по предоставлению вычислительных мощностей (договор о размещении на ресурсе, облаке) в случае, если информационная система (информационный ресурс) размещена на коммерческом ресурсе;

порядок работы или положение об информационной системе (информационном ресурсе) (при наличии).

11. По результатам рассмотрения полученной информации Министерство жилищно-коммунального хозяйства, энергетики, цифровизации и связи Забайкальского края в течение одного рабочего дня со дня ее получения принимает решение о необходимости совершения конкретных действий и информирования Управления Федеральной службы безопасности Российской Федерации по Забайкальскому краю о несанкционированном воздействии.

IV. Обязанности участников информационного взаимодействия

12. Обязанностями пользователя являются:

предоставление своего автоматизированного рабочего места администратору безопасности для контроля;

выполнение требований и рекомендаций администратора безопасности и системного администратора;

незамедлительное информирование администратора безопасности и системного администратора обо всех выявленных нарушениях, связанных с информационной безопасностью и обнаружением нештатного режима работы информационных систем и сетей.

13. Обязанностями системного администратора являются:

обеспечение бесперебойной работы системного программного обеспечения, серверного оборудования и автоматизированных рабочих мест пользователей;

обеспечение резервного копирования данных (восстановление данных при необходимости);

незамедлительное информирование администратора безопасности обо всех выявленных нарушениях, связанных с информационной безопасностью;

осуществление мероприятий по предотвращению

несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

предотвращение незаконного вмешательства в информационные ресурсы и системы в иных формах;

выполнение требований и рекомендаций администратора безопасности;

ведение журнала учета инцидентов информационной безопасности, составленного по форме согласно приложению, к настоящему Порядку;

принятие в течение 1 рабочего дня мер по восстановлению работоспособности информационных ресурсов и информационных систем, согласуемых с администратором безопасности и вышестоящим руководством (при необходимости);

проведение совместно с администратором безопасности анализа зарегистрированных инцидентов информационной безопасности с целью разработки мероприятий (плана мероприятий) по их предотвращению.

14. Обязанностями администратора безопасности являются:

проведение инструктажа пользователей по вопросам информационной безопасности;

обеспечение функционирования установленных систем защиты информации;

обновление антивирусных баз;

осуществление контроля за резервным копированием информации, сроками действия сертификатов соответствия средств защиты информации, ведением журнала учета инцидентов информационной безопасности;

проведение не реже 1 раза в год внутреннего аудита информационной безопасности;

осуществление совместно с системным администратором при получении информации об инцидентах информационной безопасности мероприятий по предотвращению несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и системы;

информирование непосредственного руководителя обо всех инцидентах, повлекших выход из строя либо временную приостановку работоспособности автоматизированных рабочих мест, автоматизированных систем и государственных информационных систем (информационных ресурсов, серверного оборудования), а также о фактах несанкционированного воздействия, заражения вредоносными программами;

проведение совместно с системным администратором анализа зарегистрированных инцидентов информационной безопасности с целью разработки плана мероприятий по их предотвращению.

V. Ответственность участников информационного взаимодействия

15. Каждый участник информационного взаимодействия несет персональную ответственность за:

свои действия во время информационного взаимодействия в рамках своих служебных обязанностей;

соблюдение требований, установленных настоящим Порядком.

Системный администратор, администратор безопасности и пользователи несут персональную ответственность за неисполнение или исполнение не в полном объеме своих обязанностей, указанных в разделе IV настоящего Порядка.

Приложение
к порядку реагирования на компьютерные
инциденты, связанные
с совершением компьютерных атак
и внедрением вредоносного
программного обеспечения в администрации
Кыринского муниципального округа

Журнал учета инцидентов информационной безопасности

N п/п	Краткое описание инцидента ИБ	Кем обнаружен (ФИО. должность)	Дата и время обнаружения	Дата и время решения проблемы	Подпись системного администратора /АИБ