АДМИНИСТРАЦИЯ КУЙБЫШЕВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

ПОСТАНОВЛЕНИЕ

«05» декабря 2025 г. № 218-п

пгт Розовка

ОБ УТВЕРЖДЕНИИ РЕГЛАМЕНТА РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ, СВЯЗАННЫЕ С СОВЕРШЕНИЕМ КОМПЬЮТЕРНЫХ АТАК И ВНЕДРЕНИЕМ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В АДМИНИСТРАЦИИ КУЙБЫШЕВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

В соответствии с Федеральным законом от 20.03.2025 г. № 33-ФЗ «Об общих принципах организации местного самоуправления в единой системе публичной власти», статьями 6, 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Уставом муниципального образования «Куйбышевский муниципальный округ Запорожской области», в целях совершенствования системы защиты информации в органах местного самоуправления, обеспечения информационной безопасности и организации порядка реагирования на события информационной безопасности, Администрация Куйбышевского муниципального округа,

ПОСТАНОВЛЯЕТ:

1. Утвердить Регламент реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения в Администрации Куйбышевского муниципального округа (далее - Регламент), в соответствии с приложением 1 к настоящему постановлению.

2. Возложить обязанности по реагированию на инциденты информационной безопасности на главного специалиста отдела организационной работы, внутренней политики и приема граждан – Вильчака Игоря Владимировича.

3. Настоящее постановление вступает в силу со дня его подписания.

4. Контроль за исполнением настоящего постановления оставляю за собой.

Глава Куйбышевского муниципального округа **К.Г. Белов**

Приложение 1
к постановлению администрации
Куйбышевского муниципального
округа от 05.12.2025 № 218-п

РЕГЛАМЕНТ
реагирования на компьютерные инциденты, связанные с совершением компьютерных атак и внедрением вредоносного программного обеспечения в Администрации Куйбышевского муниципального округа

РАЗДЕЛ I.
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент устанавливает порядок действий при возникновении угроз информационной безопасности, обусловленных возможностью несанкционированного доступа к государственным 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.

Регламент разработан для Администрации Куйбышевского муниципального округа (далее - Администрация);

1.2. В настоящем Регламенте 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, специалист по информационной безопасности (далее - администратор безопасности).

1.3. Действие положений настоящего Регламента распространяется на деятельность Администрации и обязательны к соблюдению всеми сотрудниками, участвующих в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности.

1.4. Задачами настоящего Регламента являются:

организация деятельности сотрудников Администрации осуществляющих администрирование информационных систем;

определение порядка работы пользователей, системных администраторов и администраторов безопасности;

обеспечение целостности, конфиденциальности и доступности информации;

соблюдение требований правовых актов в области защиты информации.

РАЗДЕЛ II.
ИСТОЧНИКИ И ВИДЫ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Источниками информации об инцидентах информационной безопасности в Администрации являются:

факты, выявленные сотрудниками Администрации;

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 цифрового развития, массовых коммуникаций и связи Запорожской области (далее – Минцифры Запорожской области);

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.

2.2. Основными видами инцидентов информационной безопасности в Администрации являются:

несанкционированный доступ к информационным ресурсам Администрации;

превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников Администрации;

компрометация учетных записей или паролей;

вирусная атака или вирусное заражение;

сетевые атаки.

РАЗДЕЛ III.
АНАЛИЗ ИСХОДНОЙ ИНФОРМАЦИИ

3.1 При получении информации о несанкционированном воздействии на информационную систему и сеть администратор безопасности обязаны убедиться, что инцидент информационной

безопасности не является результатом их собственной ошибки или санкционированных действий.

3.2. При выявлении инцидента информационной безопасности в Администрации администратору 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.

3.3. Администратору безопасности информационной системы, подвергшейся несанкционированному воздействию, необходимо в течение трех рабочих дней с момента обнаружения несанкционированного воздействия представить в Минцифры Запорожской области результаты служебной проверки и информацию о последствиях несанкционированного воздействия и принятых мерах по устранению причин несанкционированного воздействия.

3.4.. Совместно с результатами служебной проверки администратор безопасности также должен представить в Минцифры Запорожской области:

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) 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).

РАЗДЕЛ IV.
ОБЯЗАННОСТИ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

4.1. Обязанностями пользователя являются:

предоставление своего автоматизированного рабочего места администратору безопасности для контроля;

выполнение требований и рекомендаций администратора безопасности;

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

4.2. Обязанностями администратора безопасности являются:

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

обеспечение резервного копирования данных (восстановление данных при необходимости);

незамедлительное информирование 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;

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

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

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

проведение инструктажа пользователей по вопросам информационной безопасности;

обеспечение функционирования установленных систем защиты информации;

обновление антивирусных баз;

осуществление контроля за резервным копированием информации и сроками действия сертификатов соответствия средств защиты информации;

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

осуществление 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 анализа зарегистрированных инцидентов информационной безопасности с целью разработки плана мероприятий по их предотвращению.

РАЗДЕЛ V.
ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

5.1. Каждый участник информационного взаимодействия несет персональную ответственность за:

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

соблюдение требований, установленных настоящим Регламентом.

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

Приложение
к Регламенту
реагирования на компьютерные
инциденты, связанные
с совершением компьютерных атак
и внедрением вредоносного
программного обеспечения

ЖУРНАЛ
учета инцидентов информационной безопасности

№ п/п	Краткое описание инцидента ИБ	Кем обнаружен (ФИО. должность)	Дата и время обнаружения	Дата и время решения проблемы	Подпись Администратора безопасности