Городской округ Архангельской области
«Мирный»
АДМИНИСТРАЦИЯ МИРНОГО

П О С Т А Н О В Л Е Н И Е

«29» сентября 2023 г. № 1577

г. Мирный

Об утверждении Положения о реагировании на инциденты информационной безопасности в администрации Мирного и подведомственных ей учреждениях

В соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», статьей 31 Устава городского округа Архангельской области «Мирный» администрация Мирного **постановляет:**

1. Утвердить Положение о реагировании на инциденты информационной безопасности в администрации Мирного и подведомственных ей учреждениях (приложение к настоящему распоряжению).

2. Настоящее постановление подлежит размещению на официальном сайте городского округа Архангельской области «Мирный»в информационно-телекоммуникационной сети «Интернет».

3. Контроль исполнения настоящего постановления возложить на первого заместителя главы Мирного Бикуса Н.Л.

И.о. главы Мирного Н.Л. Бикус

Приложение
УТВЕРЖДЕНО
постановлением администрации Мирного
от «29» сентября2023 г. № 1577

ПОЛОЖЕНИЕ
о реагировании на инциденты информационной безопасности в администрации Мирного и подведомственных ей учреждениях

I. Общие положения

1. Настоящее Положение о реагировании на инциденты информационной безопасности в администрации Мирного и подведомственных ей учреждениях(далее - Положение) определяет единый и обязательный порядок реагирования на возникшие инциденты информационной безопасности, целью которого является повышение уровня защищенности информационных ресурсов администрации Мирного и подведомственных ей учреждений, за счет эффективного управления и определение порядка расследования инцидентов информационной безопасности, своевременное оповещение пользователей вычислительной сети администрации Мирного и подведомственных ей учреждений о возникающих угрозах компьютерной безопасности, распространение информации по их предупреждению, а также проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов информационной безопасности (далее – инцидент).

2. Процесс расследования и реагирования на инцидент проявляет конкретные уязвимости информационной системы, обнаруживает следы атак и вторжений, а также проверяется работа защитных механизмов, качество архитектуры системы обеспечения информационной безопасности и ее управления.

II. Термины и определения

3. Основные термины и определения, используемые в настоящем Положении:

1) инцидент информационной безопасности – событие, в результате наступления которого нанесен ущерб: финансовый, операционный и репутационный рисков (атака на информационные ресурсы учреждения, разглашение конфиденциальной информации, нарушение работоспособности информационных систем, внесение несанкционированных изменений, утечка или разглашение персональных данных и т.д.);

2) журнал регистрации событий – электронный журнал, содержащий записи о действиях пользователей и событиях в автоматизированной системе;

3) информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств её обработки;

4) событие – возникновение специфического набора обстоятельств;

5) событие информационной безопасности – идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью;

6) конфиденциальность – свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц;

7) целостность – неизменность информации в процессе ее передачи или хранения;

8) доступность – свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по

требованию уполномоченных лиц;

9) безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы;

10) ущерб имущественный – убытки, непредвиденные расходы, утрата имущества и денег, недополученная выгода;

11) угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность.

III. Порядок регистрации

4.Источником информации об инциденте информационной безопасности может служить:

сообщения сотрудников администрации Мирного и подведомственных ей учреждений, контрагентов, направленные в администрацию Мирного в виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.;

уведомления (сообщения) органов, осуществляющих контроль или надзор за деятельностью администрации Мирного и подведомственных ей учреждениях;

данные, полученные на основании анализа журналов регистрации информационных систем, систем защиты;

результаты работы средств защиты;

результаты внутренних проверок.

5. Муниципальные служащие всех отраслевых органов администрации Мирного и сотрудники подведомственных ей учреждений, отвечающие за соответствующие технологические процессы, обязаны при получении информации обо всех нетипичных событиях сообщать специалисту по

защите информации (далее – администратор по безопасности).

При получении сообщения об инциденте информационной безопасности по электронной почте или по телефону необходимо убедиться в достоверности полученной информации (например, путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных указанных в подписи сообщения или названных при звонке).

6.Администратор по безопасности сообщает главе Мирного и начальнику отраслевого органа, в котором случился инцидент.

7. Администратор по безопасности регистрирует полученную информацию в журнале учета инцидентов.

После получения информации он должен классифицировать инцидент по категории критичности, используя 4 разновидности категорий критичности инцидентов:

1 категория – инцидент может привести к значительным негативным последствиям (ущербу) для информационных ресурсов или репутации учреждения;

2 категория – инцидент может привести к негативным последствиям (ущербу) для информационных ресурсов или репутации учреждения;

3 категория – инцидент может привести к незначительным негативным последствиям (ущербу) для информационных ресурсов или репутации учреждения;

4 категория – инцидент не может привести к негативным последствиям (ущербу) для информационных ресурсов или репутации учреждения.

8. В зависимости от присвоенной категории критичности инцидента происходит определение приоритета и времени реагирования по каждому типу инцидента информационной безопасности. Сопоставление приоритетов и категорий инцидентов информационной безопасности определяется следующим образом:

очень высокий – соответствует 1 категории, время реагирования – не более 1 часа с момента классификации;

высокий – соответствует 2 категории, время реагирования – не более 4 часов с момента классификации;

средний – соответствует 3 категории, время реагирования – не более 8 часов с момента классификации;

низкий – соответствует 4 категории, время реагирования – не требует.

9. Глава Мирного доводит информацию об инциденте должностным лицам министерства связи и информационных технологий Архангельской области, а также регионального управления ФСБ России по Архангельской области.

IV. Порядок разбора

10. Для разбора инцидентов информационной безопасности создается постоянно действующая комиссия по реагированию на инциденты информационной безопасности.

11. В состав комиссии входят:

первый заместитель главы Мирного;

администратор по безопасности;

начальник отдела информационных технологий;

начальник учреждения, в котором произошел инцидент, либо лицо исполняющее его обязанности;

лицо, ответственное за организацию обработки персональных данных.

12. Комиссия анализирует все данные об обстоятельствах инцидента (электронные письма, логины информационных систем, показания сотрудников и др.). Проверяются все собранные данные о том, что произошло, когда произошло, кто совершил неприемлемые действия, и как все это может быть предупреждено в будущем.

13. Комиссия обязана установить имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и

условия, способствовавшие нарушению.

14. По окончании разбора инцидента информационной безопасности комиссией оформляется акт, в котором указываются основные события инцидента. Акт составляется по форме, приведенной в приложении к настоящему Положению.

15. Акт предоставляется главе Мирного на подпись. В конце акта указывается причина возникновения инцидента и предложения по недопущению подобных инцидентов в будущем.

16. После окончания расследования комиссия выдает рекомендации о привлечении виновных лиц к ответственности, применении защитных механизмов и проведении изменений в процедурах информационной безопасности.

17. Обеспечение деятельности комиссии по реагированию на инциденты информационной безопасности осуществляется администратором по безопасности.

V. Анализ причин и оценка результата

18. После проведения расследования комиссия по реагированию на инциденты информационной безопасности осуществляет:

переоценку рисков, повлекших возникновение инцидента;

разрабатывает перечень защитных мер для минимизации выявленных рисков, в случае повторения инцидента информационной безопасности;

актуализирует необходимые политики, регламенты, инструкции по информационной безопасности, включая настоящий документ;

организует обучение сотрудников учреждения для повышения осведомленности в области защиты информации.

Приложение
к Положению о реагировании
на инциденты информационной
безопасности администрации Мирного

АКТ № ____
об инциденте информационной безопасности

"_____"_____20____года Руководителю подразделения

1. Наименование подразделения, ФИО сотрудника, занимаемая должность:
_____
_____
(*допустившего отклонения, собирающегося совершить или совершившего операции, попадающие по признакам под инцидент*)

2. Факты установленных нарушений или возникших подозрений по поводу возможных отклонений в выполнении операций от установленных стандартов, норм, и правил с указанием даты совершения операций:
_____
_____
_____
_____
_____

Категория инцидента: _____

Информация о принятых мерах:
_____
_____
_____
_____
_____

"____"_____20_____г.

Глава Мирного _____

И.О. Фамилия

Ф.И.О. исполнителя