**Муниципальное образование сельское поселение Болчары**

**Кондинский район Ханты – Мансийский автономный округ – Югра**

**АДМИНИСТРАЦИЯ**

**сельскоГО поселениЯ Болчары**

**РАСПОРЯЖЕНИЕ**

от 24 марта 2020 года № 38 – р

с. Болчары

|  |
| --- |
| Об утверждении Положения о порядке выявления и реагирования на инциденты информационной безопасности в администрации сельского поселения Болчары |

В соответствии с федеральными законами от 27 июля 2006 года № 149 – ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 03 ноября 1994 года № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии», приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащихся в государственных информационных системах», с целью установления порядка управления инцидентами, способными привести к сбоям или нарушению функционирования информационных систем или возникновению угроз безопасности конфиденциальной информации администрации городского поселения Кондинское:

1. Утвердить Положение о порядке выявления и реагирования на инциденты информационной безопасности в администрации сельского поселения Болчары (приложение).

2. Распоряжение разместить на официальном сайте органов местного самоуправления муниципального образования Кондинский район.

3. Контроль за выполнением настоящего распоряжения возложить на заместителя главы сельского поселения Болчары.

Глава сельского поселения Болчары С. Ю. Мокроусов

Приложение

к распоряжению администрации

сельского поселения Болчары

от 24.03.2020 № 38 – р

Положение о порядке выявления и реагирования   
на инциденты информационной безопасности в администрации

сельского поселения Болчары

Статья 1. Общие положения

* 1. Настоящее Положение о порядке выявления и реагирования на инциденты информационной безопасности в администрации сельского поселения Болчары (далее – Положение) устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационных систем (далее – ИС) администрации сельского поселения Болчары и (или) возникновению угроз безопасности конфиденциальной информации администрации сельского поселения Болчары (далее – инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима конфиденциальности (далее – служебное расследование) в администрации сельского поселения Болчары.
  2. Настоящее Положение разработано в соответствии с Положением о порядке организации и проведения работ по защите конфиденциальной информации в администрации сельского поселения Болчары.
  3. Процесс управления инцидентами ИБ включает:
  + учет и регистрацию инцидентов ИБ;
  + оповещение ответственного лица о возникновении инцидентов ИБ;
  + расследование обнаруженных инцидентов ИБ;
  + устранение причин и последствий инцидентов ИБ;
  + определение плана корректирующих и превентивных мероприятий.
  1. Требования настоящего Положения являются обязательными для выполнения всеми работниками администрации сельского поселения Болчары.

Статья 2. Учет и регистрация инцидентов информационной безопасности

* 1. Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем администрации сельского поселения Болчары.
  2. В обязательном порядке должны регистрироваться следующие события безопасности:

– попытки входа (выхода) пользователей в операционную систему (из операционной системы);

* + загрузка и инициализация операционной системы и ее программного останова для рабочих станций и серверов;
  + попытка доступа к средствам виртуализации;
  + факт изменения конфигурации средств виртуализации;
  + запуск и остановка служб (системных сервисов) средств виртуализации;
  + попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.
  1. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:
  + тип события;
  + дата и время события;
  + результат события;
  + источник события;
  + идентификатор пользователя информационной системы, предъявленный при попытке доступа.
  1. Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.
  2. Учет инцидентов ИБ осуществляется администраторами ИС администрации сельского поселения Болчары (далее – администраторы ИС), назначенным распоряжением администрации сельского поселения Болчары. Допускается ведение учета инцидентов ИБ в электронном виде.
  3. При обнаружении инцидента ИБ администратор ИС проводит его классификацию в соответствии с приложением 1 к настоящему Положению. Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

Статья 3. Порядок оповещения ответственного лица о возникновении инцидентов информационной безопасности

Средства защиты информации должны обеспечивать возможность информирования администратора ИС о критических событиях безопасности в информационной системе.

В случае, если зафиксированный инцидент ИБ был классифицирован как «значимый» или «имеющий признаки компьютерного преступления», администратор ИС обязан незамедлительно сообщить о выявленном инциденте ИБ администратору информационной безопасности в администрации сельского поселения Болчары (далее – АИБ).

АИБ должен провести внеплановый анализ выявленного инцидента ИБ и, в случае необходимости, инициировать процедуру служебного расследования в соответствии с порядком, установленным данным Положением.

Статья 4. Порядок расследования обнаруженных инцидентов   
информационной безопасности

Проведение служебного расследования инициируется заместителем главы сельского поселения Болчары – ответственным за организацию и руководство работами по защите конфиденциальной информации (далее – ответственный за организацию и руководство работами). В этом же распоряжении устанавливается состав Комиссии для проведения служебного расследования (далее – Комиссия).

Служебное расследование может быть возбуждено:

* + по решению ответственного за организацию и руководство работами;
  + по инициативе любого работника администрации сельского поселения Болчары на основании служебной записки в произвольной форме на имя ответственного за организацию и руководство работами;
  + по устному докладу АИБ.

В состав Комиссии входят следующие работники администрации сельского поселения Болчары:

* + председатель Комиссии – АИБ;
  + администратор ИС.

В случае необходимости Комиссия вправе привлекать к расследованию:

* + руководителя структурного подразделения, в котором произошел инцидент ИБ;
  + экспертов из других структурных подразделений и, при необходимости, представителей сторонних организаций.

Комиссия для проведения служебного расследования в рабочем порядке в максимально короткие сроки, привлекая все необходимые ресурсы, проводит служебное расследование.

Результаты работы Комиссии оформляются в виде аналитического заключения на имя главы сельского поселения Болчары, с предложениями:

* + по внесению изменений в организационные и (или) технические меры по защите конфиденциальной информации;
* по внесению изменений и улучшений в комплект организационно-распорядительной документации администрации сельского поселения Болчары;
* по расширению или дополнению списка инцидентов ИБ, установленного данным Положением, если это необходимо.

В аналитическом заключении должен быть приведен перечень ответственных за выполнение запланированных работ и сроки выполнения запланированных работ.

Материалы служебного расследования, его выводы и заключения могут быть использованы как основание для реализации уголовной, гражданской, административной или дисциплинарной ответственности, в порядке, определяемом действующим законодательством и локальными правовыми актами администрации сельского поселения Болчары.

Статья 5. Устранение причин и последствий инцидентов   
информационной безопасности

* 1. Для инициирования работ по устранению причин и последствий инцидентов ИБ АИБ направляет аналитическое заключение ответственному за организацию и руководство работами и ответственным за выполнение запланированных работ.

Если ответственный за выполнение запланированных работ не согласен с установленными сроками, он вправе обратиться к АИБ с просьбой о переносе срока с обоснованием причин.

При изменении сроков реализации действий, АИБ вносит необходимые изменения в заключение и информирует о них ответственного за выполнение запланированных работ и ответственного за организацию и руководство работами.

* 1. После реализации запланированных работ ответственное лицо должно направить АИБ подтверждение выполнения работ, не позднее срока реализации, установленного в заключении.
  2. АИБ вправе запросить у назначенного лица информацию о выполнении в случае, если ему не поступило подтверждение выполнения работ в течение двух рабочих дней с даты, установленной в заключении.
  3. Оценку результативности предпринятых мер осуществляет АИБ на основании анализа информации, содержащейся в отчетах о проведении служебного расследования и в сводном отчете об инцидентах ИБ.
  4. О результативности предпринятых корректирующих и превентивных мер свидетельствует отсутствие повторных инцидентов ИБ.

Статья 6. Определение плана корректирующих и превентивных мероприятий

1. При выявлении инцидентов ИБ администратор ИС готовит сводный отчет за месяц по инцидентам ИБ, предоставляемый АИБ.
2. В сводном отчете администратор ИС должен провести анализ выявленных инцидентов ИБ, в качестве приложения к отчету должен быть предложен перечень корректирующих и превентивных мероприятий, направленных на устранение причин и последствий инцидентов ИБ и на предотвращение подобных нарушений в будущем. Данный перечень должен устанавливать сроки реализации и ответственных за проведение указанных мероприятий.
3. После согласования указанного перечня с АИБ, данная информация доводится администратором ИС до всех работников, назначенных ответственными за проведение корректирующих и превентивных мероприятий.
4. Контроль за своевременным и качественным выполнением работ по проведению корректирующих и превентивных мероприятий осуществляет АИБ.

Статья 7. Ответственность

1. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет АИБ.
2. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет администратор ИС, назначенный распоряжением администрации сельского поселения Болчары.

Приложение

к Положению о порядке выявления и реагирования на инциденты информационной безопасности в администрации сельского поселения Болчары

Перечень инцидентов информационной безопасности

в администрации сельского поселения Болчары

|  |  |
| --- | --- |
| №  п/п | Описание инцидента информационной безопасности |
| 1 | 2 |
| Текущие нарушения | |
|  | Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) менее трех раз подряд (однократная) |
|  | Периодические попытки неудачного доступа к объектам: компьютерам, принтерам, файлам, документам |
|  | Несанкционированный перевод времени на рабочей станции либо на других элементах информационной инфраструктуры |
|  | Выполнение производственных обязанностей с использованием компьютерного оборудования в нерабочее время |
|  | Оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время |
|  | Перезагрузка рабочей станции при сбоях в работе (однократная), в том числе аварийная перезагрузка путем нажатия кнопки горячей перезагрузки или полного отключения питания |
|  | Нецелевое использование элементов информационной инфраструктуры (печать, сервисы сети Интернет, электронная почта, и т.п.) |
| Значимые нарушения | |
|  | Ошибка при регистрации в информационной системе: ввод неправильных персональных регистрационных данных (пароля, имени пользователя и т.п.) более трех раз подряд (многократная) |
|  | Неоднократное оставление работающего (включенного) компьютерного оборудования без запущенного хранителя экрана в нерабочее время |
|  | Утрата учтенного магнитного, оптического или иного носителя конфиденциальной информации |
|  | Утрата носителя информации с резервной копией |
|  | Неудачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) (многократная) |
|  | Удачная попытка регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) |
|  | Нерегламентированная очистка журналов событий безопасности информационных систем |
|  | Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации |
|  | Нерегламентированное изменение аппаратной конфигурации компьютерного оборудования |
|  | Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.п.) и других сервисов сети Интернет |
|  | Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах |
|  | Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем (повышение уровня прав доступа, получение прав на отладку программ и т.п.) |
|  | Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное) |
|  | Нерегламентированное использование сканирующего (на различные уязвимости) программного обеспечения |
|  | Нерегламентированное использование анализаторов протоколов (снифферов) |
|  | Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите) |
|  | Несанкционированное проведение обновления версий системного и прикладного программного обеспечения |
| Нарушения, имеющие признаки преступления | |
|  | Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры администрации сельского поселения Болчары |
|  | Несанкционированное изменение конфигурации элементов информационной инфраструктуры администрации сельского поселения Болчары |
|  | Утрата резервных копий |
|  | Утечка конфиденциальной информации (баз данных информационных систем и др.) |
|  | Подозрение в умышленном нарушении работоспособности информационной сети, элементов информационной инфраструктуры, системного и прикладного программного обеспечения администрации сельского поселения Болчары |
|  | Юридически необоснованная передача (распространение) конфиденциальной информации |
|  | Несанкционированное внесение изменений в базы данных информационных систем |
|  | Несанкционированное уничтожение конфиденциальной информации |
|  | Проведение обновления версии информационных систем (равно как и другого программного обеспечения), повлекшее за собой потерю конфиденциальной информации |
|  | Намеренное заражение информационных систем администрации сельского поселения Болчары вредоносным кодом |