**Муниципальное казенное учреждение администрация**

**Нововасюганского сельского поселения**

**Каргасокского района Томской области**

**РАСПОРЯЖЕНИЕ**

19.08.2019 г. № 128

с. Новый Васюган

|  |
| --- |
| Об утверждении Порядка работы с инцидентами информационной безопасности в МКУ администрации Нововасюганского сельского поселения  |

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», [постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных](http://docs.cntd.ru/document/902377706)»,

1. Назначить ответственным ответственными за выявление инцидентов информационной безопасности в МКУ администрации Нововасюганского сельского поселения техника-программиста МКУ администрации Нововасюганского сельского поселения – Дюдяеву Ирину Александровну.

2. Утвердить Порядок работы с инцидентами информационной безопасности в МКУ администрации Нововасюганского сельского поселения, согласно приложению к настоящему распоряжению.

3. Воробьевой И.В., главному специалисту МКУ администрации Нововасюганского сельского поселения ознакомить с настоящим распоряжением всех работников МКУ администрации Нововасюганского сельского поселения, осуществляющих обработку персональных данных, под роспись.

Глава Нововасюганского

сельского поселения П.Г. Лысенко

И.В. Воробьева

8 (38253) 29393

Приложение № 1

Порядка работы с инцидентами информационной безопасности в МКУ администрации Нововасюганского сельского поселения

1. Общие положения

1.1. Порядок работы с инцидентами информационной безопасности в МКУ администрации Нововасюганского сельского поселения разработан в целях выявления угроз информационной безопасности, определения порядка действий пользователей информационных систем и повышения общего уровня защищенности информационных ресурсов и информационных систем.

Настоящий Порядок разработан в соответствии с [Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных](http://docs.cntd.ru/document/901990046)», [Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»](http://docs.cntd.ru/document/901990051), [Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»](http://docs.cntd.ru/document/902377706), [Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»](http://docs.cntd.ru/document/499005278), [Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»](http://docs.cntd.ru/document/499002630).

1.2. Инцидент информационной безопасности - одно событие или группа событий, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности, в том числе при обработке персональных данных.

Инциденты информационной безопасности могут быть преднамеренными или случайными и могут вызываться как техническими, так и физическими средствами. Их последствиями могут быть такие события, как несанкционированное изменение информации, ее уничтожение или другие события, которые сделают информацию недоступной.

1.3. К инцидентам информационной безопасности относятся:

разглашение информации ограниченного распространения, не составляющей государственную тайну (далее - защищаемая информация);

передача защищаемой информации по открытым каналам связи;

передача носителя защищаемой информации лицу, не имеющему права доступа к ней;

утрата или хищение носителя с защищаемой информацией;

несанкционированное изменение, копирование защищаемой информации;

несанкционированный доступ к информационным системам.

1.4. Работа с инцидентами информационной безопасности включает в себя следующие направления:

определение лиц, ответственных за выявление инцидентов и реагирование на них;

обнаружение, идентификация и регистрация инцидентов;

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

принятие мер по устранению последствий инцидентов;

планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2. Ответственные за реагирование на инциденты в информационной безопасности

2.1. Ответственными за реагирование на инциденты в информационной системе являются:

работники МКУ администрации Нововасюганского сельского поселения, имеющие право доступа к информационной системе;

Глава Нововасюганского сельского поселения;

администратор информационной безопасности;

работник МКУ администрации Нововасюганского сельского поселения, ответственный за организацию обработки персональных данных, в случае, если информационная система является информационной системой персональных данных.

3. Порядок действий при возникновении инцидентов информационной безопасности

3.1. Работа по обнаружению инцидентов информационной безопасности включает в себя мероприятия, направленные на выявление инцидентов в области информационной безопасности с помощью технических средств, в ходе контрольных мероприятий.

3.2. Работник МКУ администрации Нововасюганского сельского поселения, обнаруживший инцидент в информационной системе, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственно Главе Нововасюганского сельского поселения, администратору информационной безопасности, работнику МКУ администрации Нововасюганского сельского поселения, ответственному за организацию обработки персональных данных (в случае, если информационная система является информационной системой персональных данных).

3.3. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий осуществляет администратор информационной безопасности.

3.4. Меры по устранению последствий инцидентов включают в себя мероприятия, направленные на определение границ инцидента и ущерба от реализации угроз информационной безопасности, а также на ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

3.5. Оценка последствий инцидента производится на основании потенциально возможного ущерба.

4. Оформление результатов проведенного разбирательства

4.1. Собранная в процессе разбирательства информация фиксируется в картотеке данных «Инциденты информационной безопасности» (согласно приложения № 1 к Порядку работы с инцидентами информационной безопасности в МКУ администрации Нововасюганского сельского поселения) и учитывается при подготовке итогового заключения по инциденту информационной безопасности.

4.2. Осуществляющий разбирательство сотрудник формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента информационной безопасности.

4.3. Итоговое заключение по инциденту информационной безопасности осуществляющий разбирательство сотрудник направляет Главе Нововасюганского сельского поселения.

4.4. Осуществляющий разбирательство сотрудник фиксирует завершение разбирательства в карточке «Инциденты информационной безопасности» и присваивает инциденту статус «Разбирательство завершено».

5. Завершение разбирательства

5.1. По завершению разбирательства инцидента информационной безопасности, осуществляющий разбирательство сотрудник передает имеющиеся материалы (в объеме, достаточном для принятия решения) Главе Нововасюганского сельского поселения для решения вопроса о целесообразности привлечения нарушителя информационной безопасности к дисциплинарной ответственности.

5.2. На основании полученных результатов разбирательства Главе Нововасюганского сельского поселения, в срок не более 3 (трех) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:

анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя информационной безопасности;

проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

6. Права, обязанности и ответственность участников разбирательства

6.1. Осуществляющий разбирательство сотрудник имеет право:

- по согласованию с Главой Нововасюганского сельского поселения требовать предоставлений письменных объяснений по обстоятельствам инцидента информационной безопасности у нарушителя информационной безопасности;

- запрашивать и получать устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента информационной безопасности;

- инициировать процедуры привлечения нарушителя информационной безопасности к дисциплинарной ответственность.

6.2. Осуществляющий разбирательство сотрудник обязан:

- объективно и основательно проводить разбирательство каждого инцидента информационной безопасности;

- определять первоочередные меры, направленные на локализацию инцидента информационной безопасности и минимизацию негативных последствий;

- фиксировать в карточке данных «Инциденты информационной безопасности» всю исходную информацию об инциденте информационной безопасности и результаты его расследования;

- предоставлять отчеты и рекомендации по проведенным разбирательствам Главе Нововасюганского сельского поселения.

- проводить анализ обстоятельств, способствовавших совершению каждого инцидента информационной безопасности, и на его основе, разрабатывать рекомендации и предложения по оптимизации процессов и снижения ущерба от подобных инцидентов информационной безопасности и минимизации возможности их повторения в будущем;

- составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

6.3. Работники МКУ администрации Нововасюганского сельского поселения обязаны:

- предоставлять по запросам проводящего разбирательство сотрудника устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента информационной безопасности;

- информировать о выявленных инцидентах информационной безопасности;

- информировать об имеющихся запросах и обращениях субъектов персональных данных.

Приложение

к Порядку работы с инцидентами информационной безопасности в МКУ администрации Нововасюганского сельского поселения

Карточка данных о инциденте информационной безопасности.

|  |  |  |  |
| --- | --- | --- | --- |
| Дата события |  |  | Стр. 1 |
| Номер события[[1]](#footnote-1)): |  | (Если требуется) соответствующие идентификационные номера событий и (или) инцидентов: |  |
| Информация о сообщающем лице |
| Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Адрес | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Организация | \_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Телефон | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Электронная почта | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Описание события информационной безопасности |
| Описание события: |
| Что произошло |  |
| Как произошло |  |
| Почему произошло |  |
| Пораженные компоненты |  |
| Негативное воздействие на бизнес |  |
|  Любые идентифицированные уязвимости |  |
| Детали события информационной безопасности  |
| Дата и время возникновения события |  |
| Дата и время обнаружения события  |  |
| Дата и время сообщения о событии |  |
| Закончилось ли событие? (отметить квадрат) | Да  Нет  |
| Если «да», то уточнить, как долго длилось событие в днях/часах/минутах |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Дата инцидента |  |  | Стр. 2 |
| Номер инцидента[[2]](#footnote-2)): |  | (Если требуется) соответствующие идентификационные номера событий и (или) инцидентов: |  |
| Информация о сотруднике группы обеспечения эксплуатации |
| Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Адрес | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Телефон | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Электронная почта | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Информация о сотруднике ISIRT |
| Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Адрес | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Телефон | \_\_\_\_\_\_\_\_\_\_\_\_\_ | Электронная почта | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Описание инцидента информационной безопасности  |
| Дальнейшее описание инцидента: |
| Что произошло |  |
| Как произошло |  |
| Почему произошло |  |
|  Пораженные компоненты |  |
|  Негативное воздействие на бизнес |  |
| Любые идентифицированные уязвимости |  |
| Детали инцидента информационной безопасности |
| Дата и время возникновения инцидента |  |
| Дата и время обнаружения инцидента |  |
| Дата и время сообщения об инциденте |  |
| Закончился ли инцидент? (отметить квадрат) | Да  Нет  |
| Если «да», то уточнить, как долго длился инцидент в днях/часах/минутах. Если «нет», то уточнить, как долго он уже длится |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Стр. 3 |
|  |  |  |  |
| Тип инцидента **информационной безопасности**  |
| (Отметить один квадрат, затем заполнить соответствующие поля ниже) | Действительный  | Попытка  | Подозрение  |
|  |
| (Один из) | Намеренная  | (указать типы угрозы) |  |
|  |
| Хищение (TH) |  | Хакерство/Логическое проникновение (HA) |  |
| Мошенничество (FR) |  | Неправильное использование ресурсов (MI) |  |
| Саботаж/физический ущерб (SA) |  | Другой ущерб (OD) |  |
| Вредоносная программа (MC) |  |  |  |
|  |  | Определить: |  |
|  |
| (Один из) | Случайная  | (указать типы угрозы) |
|  |
| Отказ аппаратуры (HF) |  | Другие природные события (NE) |  |
| Отказ ПО (SF) |  | Определить: |  |
| Отказ связи (CF) |  | Потеря существенных сервисов (LE) |  |
| Пожар (HE) |  | Недостаточное кадровое обеспечение (SS) |  |
| Наводнение (FL) |  | Другие случаи (OA) |  |
|  | Определить: |
|  |
| (Один из) | Ошибка  | (указать типы угрозы) |
|  |
| Операционная ошибка (OE) |  | Ошибка пользователя (UE) |  |
| Ошибка аппаратной поддержки (HE) |  | Ошибка конструкции (DE) |  |
| Ошибка поддержки ПО (SE) |  | Другие случаи (включая истинные заблуждения) (OA) |  |
|  | Определить: |
|  |
| Неизвестно  |  | (Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат «неизвестно» и, по возможности, указать тип угрозы, ,используя сокращения, приведенные выше) |
|  | Определить: |
|  |  |  | Стр. 4 |
|  |  |  |  |
| Пораженные активы |
| Пораженные активы (если есть) | (Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности) |
|  |
|  | Информация/Данные | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Аппаратура | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Программное обеспечение | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Средства связи | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | Документация | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |
| Негативное воздействие/влияние инцидента на бизнес |
|  |
| Отметить соответствующие квадраты для указанных ниже нарушений, затем в колонке «значимость» указать уровень негативного воздействия на бизнес по шкале 110, используя сокращения (указатели категорий): (FD) – финансовые потери/разрушение бизнес-операций, (CE) – коммерческие и экономические интересы, (PI) – информация, содержащая персональные данные, (LR) – правовые и нормативные обязательства(это необходимо сличить с английским оригиналом),(МО) – менеджмент и бизнес-операции, (LG) – потеря престижа Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость» |
|  |
|  | Значимость | Указатели | Стоимость |
|  |  |  |  |
| Нарушение конфиденциальности(т. е., несанкционированное раскрытие) |  |  |  |  |
| Нарушение целостности(т. е., несанкционированная модификация) |  |  |  |  |
| Нарушение доступности(т. е., недоступность) |  |  |  |  |
| Нарушение неотказуемости |  |  |  |  |
| Уничтожение |  |  |  |  |
|  |
| Полные стоимости восстановления после инцидента |
|  |
| (Где возможно, необходимо указать общие расходы на восстановление после инцидента в целом по шкале 110 для «значимости» и в деньгах для «стоимости») | Значимость | Указатели | Стоимость |
|  |  |  | Стр. 5 |
|  |  |  |  |
| Разрешение инцидента |
| Дата начала расследования инцидента | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Фамилия лица (лиц), проводившего (их) расследование инцидента | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата окончания инцидента | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата окончания воздействия | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата завершения расследования инцидента | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Ссылка и место хранения отчета о расследовании | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |
| Причастные лица |
|  |
| (Один из) | Лицо (PE) |  | Легально учрежденная организация/учреждение (OI) |  |
| Организованная группа (GR) |  | Случайность (AC) |  |
|  |  | Нет виновного (NP)Например, природные факторы, отказ оборудования, ошибка человека |  |
|  |
| Описание нарушителя |
|  |
| Действительная или предполагаемая мотивация |
|  |
| (Один из) | Криминальная/финансовая выгода(CG) |  | Развлечение/хакерство (PH) |  |
| Политика/Терроризм (PT) |  | Реванш (RE) |  |
|  |  | Другие мотивы (OM) |  |
|  |  | Определить: |  |
|  |
| Действия, предпринятые для разрешения инцидента |
|  |
| (например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением…») |  |
|  |
| Действия, запланированные для разрешения инцидента |
|  |
| (например, см. выше) |  |
|  |
| Прочие действия |
|  |
| (например, по-прежнему требуется проведение расследования для другого персонала) |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Стр. 6 |
|  |  |  |  |
| Заключение |
| (Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения) | Значительный  | Незначительный  |
|  |
| (Укажите любые другие заключения) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |
| Ознакомленные лица/субъекты |
|  |
| (Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия. Обычно этим лицом является руководитель ИБ организации). | Руководитель ИБ |  | Руководитель ГРИИБ |  |
| Местный руководитель (уточнить, какого подразделения) |  | Руководитель информационных систем |  |
| Автор отчета |  | Руководитель автора отчета |  |
| Полиция |  | Другое лица |  |
|  | (например, справочная служба, отдела кадров, менеджмента, внутреннего аудита, регулятивного органа, сторонняя КСБР) |
|  | Определить: |
|  |
|  |
|  |
| Привлеченные лица |
|  |
| Инициатор | Аналитик | Аналитик |
|  |
| Подпись | \_\_\_\_\_\_\_\_\_\_\_\_\_ | Подпись | \_\_\_\_\_\_\_\_\_\_\_\_ | Подпись | \_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_\_ | Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_ | Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Роль | \_\_\_\_\_\_\_\_\_\_\_\_\_ | Роль | \_\_\_\_\_\_\_\_\_\_\_\_ | Роль | \_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата | \_\_\_\_\_\_\_\_\_\_\_\_\_ | Дата | \_\_\_\_\_\_\_\_\_\_\_\_ | Дата | \_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |
|  |
|  |
| Аналитик | Аналитик | Аналитик |
|  |
| Подпись | \_\_\_\_\_\_\_\_\_\_\_\_ | Подпись | \_\_\_\_\_\_\_\_\_\_\_\_ | Подпись | \_\_\_\_\_\_\_\_\_\_\_\_ |
| Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_ | Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_ | Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_ |
| Роль | \_\_\_\_\_\_\_\_\_\_\_\_ | Роль | \_\_\_\_\_\_\_\_\_\_\_\_ | Роль | \_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата | \_\_\_\_\_\_\_\_\_\_\_\_ | Дата | \_\_\_\_\_\_\_\_\_\_\_\_ | Дата | \_\_\_\_\_\_\_\_\_\_\_\_ |

1. ) (Номера событий назначаются Главой Нововасюганского сельского поселения) [↑](#footnote-ref-1)
2. ) (Номера инцидентов назначаются Главой Нововасюганского сельского поселения) [↑](#footnote-ref-2)