ПРАВИТЕЛЬСТВО АРХАНГЕЛЬСКОЙ ОБЛАСТИ

МИНИСТЕРСТВО ТРУДА, ЗАНЯТОСТИ И СОЦИАЛЬНОГО РАЗВИТИЯ АРХАНГЕЛЬСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

от 4 октября 2023 г. № 39-п

г. Архангельск

Об утверждении положения о реагировании на инциденты информационной безопасности в министерстве труда, занятости и социального развития Архангельской области

В соответствии с пунктом 14 Положения о министерстве труда, занятости и социального развития Архангельской области, утвержденного постановлением Правительства Архангельской области от 27 марта 2012 года № 117-пп, пунктом 2.4 Протокола заочного заседания оперативного штаба по обеспечению кибербезопасности на территории Архангельской области от 25 августа 2023 года № 02-01/115 министерство труда, занятости и социального развития Архангельской области **п о с т а н о в л я е т:**

1. Утвердить прилагаемое Положение о реагировании на инциденты информационной безопасности в министерстве труда, занятости и социального развития Архангельской области.

2. Настоящее постановление вступает в силу со дня его официального опубликования.

Исполняющий обязанности министра труда, занятости и социального развития Архангельской области **В.А. Торопов**

УТВЕРЖДЕНО
постановлением министерства труда,
занятости и социального развития
Архангельской области
от 4 октября 2023 г. № 39-п

ПОЛОЖЕНИЕ
о реагировании на инциденты информационной безопасности в министерстве труда, занятости и социального развития Архангельской области

Термины и определения

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

Инцидент информационной безопасности – событие, в результате наступления которого нанесен ущерб в виде финансовых потерь, операционных и репутационных рисков (атака на информационные ресурсы учреждения, разглашение конфиденциальной информации, нарушение работоспособности информационных систем, внесение несанкционированных изменений, утечка или разглашение персональных данных и т.д.);

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

Событие – возникновение специфического набора обстоятельств;

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;

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

Целостность – неизменность информации в процессе ее передачи или хранения;

Доступность – свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц;

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;

Ущерб – убытки, непредвиденные расходы, утрата имущества и денег, недополученная выгода;

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность.

1. Область применения

1.1. Целью настоящего Положения является повышение уровня защищенности информационных ресурсов министерства, за счет эффективного управления и определение порядка расследования инцидентов информационной безопасности, своевременное оповещение пользователей вычислительной сети министерства о возникающих угрозах компьютерной безопасности, распространение информации по их предупреждению.

1.2. 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.

2. Порядок регистрации

2.1. Источником информации об инциденте информационной безопасности может служить следующее:

- сообщения государственных гражданских служащих Архангельской области и работников министерства, контрагентов направленные в министерство в виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.;
- уведомления (сообщения) органов, осуществляющих контроль или надзор за деятельностью министерства;
- данные, полученные на основании анализа журналов регистрации информационных систем, систем защиты;
- результаты работы средств защиты;
- результаты внутренних проверок.

Государственные гражданские служащие Архангельской области и работники подразделений министерства, отвечающие за соответствующие технологические процессы, обязаны при получении информации обо всех нетипичных событиях сообщать администратору безопасности информации (далее – администратор безопасности).

2.2. При получении сообщения об инциденте информационной безопасности по электронной почте или по телефонному звонку 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).

2.3. Сотрудник, получивший информацию об инциденте, должен незамедлительно сообщить об этом начальнику отдела материально-технического оснащения, государственных закупок финансово-

экономического управления министерства. Начальник отдела материально-технического оснащения, государственных закупок финансово-экономического управления министерства сообщает заместителю министра – начальнику соответствующего структурного управления, в котором случился инцидент.

2.4. Министр труда, занятости и социального развития Архангельской области доводит информацию об инциденте должностным лицам министерства связи и информационных технологий Архангельской области,
а также регионального управления ФСБ России по Архангельской области.

2.5. Администратор безопасности регистрирует полученную информацию в журнале учета инцидентов.

После получения информации работники должны классифицировать инцидент по категории критичности, используя 4 разновидности категорий критичности инцидентов:

- 1 категория – инцидент может принести к значительным негативным последствиям (ущербу) для информационных ресурсов или репутации учреждения.
- 2 категория – инцидент может принести к негативным последствиям (ущербу) для информационных ресурсов или репутации учреждения.
- 3 категория – инцидент может принести к незначительным негативным последствиям (ущербу) для информационных ресурсов или репутации учреждения.
- 4 категория – инцидент не может принести к негативным последствиям (ущербу) для информационных ресурсов или репутации учреждения.

2.6. 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 определено.

3. Порядок разбора

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

3.2. В состав комиссии входят следующие сотрудники министерства:

- министр труда, занятости и социального развития Архангельской области (председатель комиссии);
- заместитель министра – начальник управления (по согласованию);
- начальник отдела материально-технического оснащения, государственных закупок финансово-экономического управления министерства (секретарь комиссии);
- руководитель структурного подразделения, в котором произошел инцидент;
- ответственный за организацию обработки персональных данных;
- иные сотрудники, на усмотрение председателя комиссии.

3.3. Комиссия собирает и анализирует все данные об обстоятельствах инцидента (электронные письма, логи 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.

3.4. Комиссия обязана установить имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лица, виновные в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению.

3.5. По окончании разбора инцидента информационной безопасности комиссией оформляется акт, в котором указываются основные события инцидента. Акт представляется в форме, указанной в приложении к настоящему Положению.

3.6. Акт предоставляется министру труда, занятости и социального развития Архангельской области на подпись. В конце отчета указывается причина возникновения инцидента и предложения по недопущению подобных инцидентов в будущем.

3.7. После окончания расследования комиссия принимает решение о наказании виновных лиц, применении защитных механизмов и проведение изменений в процедурах информационной безопасности.

4. Анализ причин и оценка результата

4.1. После проведения расследования комиссия проводит:

- переоценку рисков, повлекших возникновение инцидента;
- готовит перечень защитных мер для минимизации выявленных рисков, в случае повторения инцидента информационной безопасности;
- актуализирует необходимые политики, регламенты, инструкции по информационной безопасности, включая настоящий документ;
- при необходимости, организует обучение сотрудников министерства для повышения осведомленности в области защиты информации.

ПРИЛОЖЕНИЕ
к Положению о реагировании на
инциденты информационной
безопасности
в министерстве труда, занятости и
социального развития
Архангельской области

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.

_____ _____
(подпись) *(фамилия и инициалы)*

Подпись и ФИО составителя: _____
Согласовано: