МИНИСТЕРСТВО ОБРАЗОВАНИЯ АРХАНГЕЛЬСКОЙ ОБЛАСТИ

Государственное автономное профессиональное образовательное учреждение Архангельской области «Архангельский политехнический техникум»

ПРИКАЗ

от 22 сентября 2023 года № 725

г. Архангельск

Об утверждении положения о реагировании на инциденты информационной безопасности в государственном автономном профессиональном образовательном учреждении Архангельской области «Архангельский политехнический техникум»

В соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», иными нормативно-правовыми актами, действующими на территории Российской Федерации

приказываю:

1.Утвердить прилагаемое Положение о реагировании на инциденты информационной безопасности в государственном автономном профессиональном образовательном учреждении Архангельской области «Архангельский политехнический техникум» (далее - Положение).

2. Положение, утвержденное в пункте 1 настоящего приказа, вступает в силу с момента его подписания.

3. Начальнику отдела цифровизации Мамонову Сергею Николаевичу под подпись ознакомить работников отдела по цифровизации, заместителей

руководителя и руководителей структурных подразделений с Положением, утвержденным в пункте 1 настоящего приказа, до 02 октября 2023 года.

4. Руководителям структурных подразделений провести работу по ознакомлению сотрудников структурных подразделений с Положением, утвержденным в пункте 1 настоящего приказа, до 10 октября 2023 года.

5. Инженеру-программисту Плосконосову Андрею Александровичу разместить Положение, утвержденное в пункте 1 настоящего приказа, на сайте учреждения до 02 октября 2023 года.

6. Контроль за исполнением приказа возложить на заместителя директора по учебно-производственной работе Афанасьеву Анжелику Викторовну.

Директор

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00E30691499EEF6F2CD14E26B0DB0DB5D5
Владелец: Ермолин Дмитрий Петрович
Действителен: с 06.02.2023 до 01.05.2024

Д.П. Ермолин

ПРИНЯТО	УТВЕРЖДЕНО
Советом государственного автономного профессионального образовательного учреждения Архангельской области «Архангельский политехнический техникум»	приказом государственного автономного профессионального образовательного учреждения Архангельской области «Архангельский политехнический техникум»
протокол № 4 от 20 сентября 2023 года	от «22» сентября 2023 года № 725

ПОЛОЖЕНИЕ
о реагировании на инциденты информационной безопасности в государственном автономном профессиональном образовательном учреждении Архангельской области «Архангельский политехнический техникум»

1. 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.

2. Область применения

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

2.2. 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.

3. Порядок регистрации

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

- сообщения работников, контрагентов направленные в учреждение в виде

сообщений по электронной почте, служебных записок, писем, заявлений и т.д.;

- уведомления (сообщения) органов, осуществляющих контроль или надзор за деятельностью учреждения;

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

- результаты работы средств защиты;

- результаты внутренних проверок.

Работники всех структурных подразделений учреждения, отвечающие за соответствующие технологические процессы, обязаны при получении информации обо всех нетипичных событиях сообщать администратору безопасности информации (далее – администратор безопасности).

3.2. 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).

3.3. Сотрудник, получивший информацию об инциденте, должен незамедлительно сообщить об этом начальнику отдела по цифровизации. Начальник отдела по цифровизации сообщает директору учреждения и руководителю структурного подразделения, в котором случился инцидент.

3.4. Директор учреждения доводит информацию об инциденте должностным лицам министерства связи и информационных технологий Архангельской области, а также регионального управления ФСБ России по Архангельской области.

3.5. 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.

3.6. 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.

4. Порядок разбора

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

4.2. В состав комиссии входят следующие сотрудники учреждения:

- директор учреждения (председатель комиссии);
- заместитель директора по административно-хозяйственной работе;
- заместитель директора по учебно-производственной работе;
- начальник отдела по цифровизации;
- руководитель структурного подразделения, в котором произошел инцидент;
- ответственный за организацию обработки персональных данных;
- иные сотрудники, на усмотрение председателя комиссии.

4.3. 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.

4.4. 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.

4.5. По окончании разбора инцидента информационной безопасности комиссией оформляется акт, в котором указываются основные события инцидента. Акт представляется в форме, указанной в Приложении 1 к настоящему Положению.

4.6. Акт предоставляется директору учреждения на подпись. В конце отчета указывается причина возникновения инцидента и предложения по недопущению подобных инцидентов в будущем.

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

5. Анализ причин и оценка результата

5.1. 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 работников учреждения для повышения осведомленности в области защиты информации.

6. Контроль исполнения настоящего положения

6.1. Контроль надлежащего исполнения требований настоящего Положения осуществляется заместителем директором учреждения.

7. Внесение изменений и дополнений

7.1. Изменения и дополнения могут вноситься в настоящее Положение по инициативе сотрудников с согласования директором по мере необходимости, но не реже чем в пять лет. Все изменения должны учитываться в листе «История изменений».

8. История изменений

Версия	Дата	Изменения	Кто внес изменения

	утверждения		
Версия	**Дата утверждения**	**Изменения**	**Кто внес изменения**

ПРИЛОЖЕНИЕ № 1
к Положению о реагировании

на инциденты информационной
безопасности в ГАПОУ АО
«Архангельский
политехнический техникум»

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:

_____