

Согласовано Советом колледжа
Председатель Совета

Пугачева /О.А.Пугачева/
«22» сентября 2023 г.

Утверждено
приказом директора ГБПОУ АО
«Архангельский
музыкальный колледж»
от 22.09.2023 № 332

ПОЛОЖЕНИЕ

о реагировании на инциденты информационной безопасности
в государственном бюджетном профессиональном образовательном учреждении
Архангельской области «Архангельский музыкальный колледж»

Содержание

Термины и определения.....	3
1. Область применения	4
2. Порядок регистрации.....	4
3. Порядок разбора	5
4. Анализ причин и оценка результата.....	5
5. Внесение изменений и дополнений.....	6
Приложение 1 к Положению	7
История изменений.....	8

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 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.

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 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 отделов учреждения, отвечающие за соответствующие технологические процессы, обязаны при получении информации обо всех нетипичных событиях сообщать администратору безопасности информации (далее – администратор безопасности). Администратором безопасности в учреждении является техник – программист.

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. Работник, получивший информацию об инциденте, должен незамедлительно сообщить об этом администратору безопасности. Администратор безопасности сообщает директору учреждения, либо лицу, его замещающему.

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

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 директором учреждения создается комиссия по реагированию на инциденты информационной безопасности.

3.2. В состав комиссии входят следующие сотрудники учреждения:

- директор учреждения (председатель комиссии);
- заместитель директора по учебно-производственной и методической работе;
- заместитель директора по административно-хозяйственной части;
- техник-программист;
- руководитель отдела, в котором произошел инцидент;
- ответственный за организацию обработки персональных данных (в случае, если инцидент связан с информационной системой персональных данных).

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 1 к настоящему Положению.

3.6. Акт предоставляется директору учреждения 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 работников учреждения для повышения осведомленности в области защиты информации.

5. Внесение изменений и дополнений

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

АКТ № _____
об инциденте информационной безопасности

" _____ " _____ 20__ года

Руководителю отдела(директору колледжа)

1. Наименование отдела, ФИО работника, 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:

