

ПОЛОЖЕНИЕ

о реагировании на инциденты информационной безопасности в государственном автономном профессиональном образовательном учреждении Пензенской области «Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»

1. Термины и определения

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

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

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.

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

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

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

2. Область применения

2.1. Целью настоящего Положения является повышение уровня защищенности информационных ресурсов образовательной организации, за счет эффективного управления и определение порядка расследования инцидентов информационной безопасности, своевременное оповещение пользователей вычислительной сети образовательной организации 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 образовательную организацию в виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.;
- уведомления (сообщения) органов, осуществляющих контроль или надзор за деятельностью образовательной организации;
- данные, полученные на основании анализа журналов регистрации информационных систем, систем защиты;
- результаты работы средств защиты;
- результаты внутренних проверок.

Работники всех структурных подразделений образовательной организации, отвечающие за соответствующие технологические процессы, обязаны при получении информации обо всех нетипичных событиях сообщать сотруднику, ответственному за обеспечение информационной 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 заместителю директора по информатизации, который в свою очередь

доводит информацию до директора образовательной организации и руководителя структурного подразделения, в котором случился инцидент.

3.4. 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 образовательной организации.
- 2 категория – инцидент может принести к негативным последствиям (ущербу) для информационных ресурсов или репутации образовательной организации.
- 3 категория – инцидент может принести к незначительным негативным последствиям (ущербу) для информационных ресурсов или репутации образовательной организации.
- 4 категория – инцидент не может принести к негативным последствиям (ущербу) для информационных ресурсов или репутации образовательной организации.

3.5. Директор образовательной организации доводит информацию об инциденте 1-й категории критичности должностным лицам Министерства образования Пензенской области.

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 инцидента информационной безопасности

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

4.2. В состав комиссии входят следующие сотрудники образовательной организации:

- директор (председатель комиссии);
- заместитель директора по информатизации;
- начальник хозяйственного отдела;

- 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, журналы информационных систем, показания сотрудников и др.), времени его наступления, лицах, совершивших действия, повлекшие возникновение инцидента, и способах недопущения и предупреждения подобных инцидентов 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 согласно форме, приведенной в Приложении 1 к настоящему Положению.

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

5. Анализ причин возникновения инцидента информационной безопасности и оценка результата

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 образовательной организации для повышения осведомленности в области защиты информации.

6. Контроль исполнения настоящего положения

- Контроль надлежащего исполнения требований настоящего Положения осуществляется директором образовательной организации.

ПРИЛОЖЕНИЕ № 1
к Положению о реагировании
на инциденты информационной безопасности
в ГАПОУ ПО ПКИПТ (ИТ-колледж)

АКТ № _____
об инциденте информационной безопасности

" _____ " _____ 20 ____ года

Члены комиссии, утвержденной приказом № _____ от « ____ » _____ 20 ____ года, рассмотрели обстоятельства инцидента информационной безопасности:

1. Содержание инцидента:

(краткое описание содержания инцидента)

2. Лицо, действия которого привели к наступлению инцидента:

(ФИО, должность, подразделение)

3. Факты установленных нарушений или возникших подозрений по поводу возможных отклонений в выполнении операций от установленных стандартов, норм, и правил с указанием даты совершения операций:

4. Категория инцидента: _____

5. Предложения по результатам рассмотрения инцидента информационной безопасности:

Председатель комиссии

_____/_____/_____
(ФИО) (Подпись) (Дата)

Члены комиссии

_____/_____/_____
(ФИО) (Подпись) (Дата)
_____/_____/_____
(ФИО) (Подпись) (Дата)
_____/_____/_____
(ФИО) (Подпись) (Дата)