МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Карачаево-Черкесский государственный университет имени У.Д. Алиева»
(КЧГУ)

Утверждаю
И.о, ректора КЧГУ
_____ Т.А. Узденов
«__» 06 2025 г.

ПОЛОЖЕНИЕ
о реагировании на компьютерные инциденты информационной безопасности

1. Термины и определения

Журнал регистрации событий - электронный журнал, содержащий записи о действиях пользователей;

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, 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 информационных систем;

Ущерб - убытки, непредвиденные расходы, утрата имущества;

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 об этом проректору по комплексной 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 проректору по комплексной безопасности, для регистрации полученной информации в журнале учета инцидентов, последующего анализа и передаче полученной информации в компетентные структуры организации и правоохранительные органы.

3.4. Регистрация полученной информации в журнале учета инцидентов осуществляется по организационному алгоритму. Алгоритм предусматривает, что после получения информации должна происходить классификация инцидента 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.

3.5. 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:

- руководитель учреждения (председатель комиссии);
- проректор по комплексной безопасности;
- проректор по учебной работе;

- начальник УАХЧ;
- начальник ЦИТ;
- 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.). 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 руководителю 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 применении защитных механизмов и при необходимости проведение изменений в процедурах информационной безопасности.

5. Анализ причин и оценка результата

5.1. После проведения расследования комиссия проводит (при необходимости, в зависимости от характера и категории инцидента):
- 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;
- 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 проректором по комплексной безопасности.

7. Внесение изменений и дополнений

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

ПРИЛОЖЕНИЕ №1
к Положению о реагировании
на инциденты информационной
безопасности в КЧГУ имени У.Д. Алиева

АКТ № _

об инциденте информационной безопасности

"____ " _____20 __ года

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:

_____ _____

(фамилия и инициалы) *(подпись)*

Подпись и ФИО составителя:

Согласовано: