Приложение № 12 к приказу
от 28.06.2019 № 01-09/315
УТВЕРЖДЕНА
приказом генерального директора
КГБОУ ХКЦВР Созвездие
от 28.06.2019 № 01-09/315

ИНСТРУКЦИЯ

по управлению инцидентами

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инциденты информационной безопасности разделены на категории:

1.1.1. Категория 1 – отказ технических средств и средств защиты информации (далее – СЗИ).

1.1.2. Категория 2 – системные сбои или перегрузки технических средств и СЗИ.

1.1.3. Категория 3 – сбои программного обеспечения.

1.1.4. Категория 4 – неконтролируемые изменения конфигурации.

1.1.5. Категория 5 – нарушение физических мер защиты информации.

1.1.6. Категория 6 – нарушение правил доступа к информации.

1.1.7. Категория 7 – несоблюдение пользователями требований организационно-распорядительной документации по защите информации.

1.1.8. Категория 8 – ошибки пользователей.

1.2. Любое событие (группа событий) информационной безопасности, приводящее к реализации или вероятности реализации любой из категорий п. 1.1. должны квалифицироваться как инциденты.

2. ПОРЯДОК ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ

2.1. Правила и порядок сбора информации о событиях информационной безопасности приведены в «Инструкции по управлению событиями информационной безопасности».

2.2. Выявление и учет инцидентов организует администратор безопасности на основе сообщений пользователей и анализа событий информационной безопасности.

2.3. Если администратор безопасности определяет текущее событие безопасности как инцидент, то он незамедлительно принимает в установленном порядке меры для устранения последствий инцидента в рамках своих полномочий.

2.4. При выявлении инцидента осуществляют оповещение пользователей об инциденте. Форму и порядок оповещения устанавливает администратор безопасности.

3. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

3.1. При реагировании на инциденты:

3.1.1. Осуществляют анализ инцидента:

3.1.1.1. Проводят оценку нанесенного материального ущерба.

3.1.1.2. Выявляют неучтенные в системе защиты информации угрозы безопасности.

3.1.1.3. Расследуют причины возникновения инцидента.

3.1.2. Устраняют причины и последствия инцидента.

3.1.3. Формируют перечень мероприятий по предотвращению инцидента в будущем.

3.2. Анализ инцидента организует администратор безопасности с привлечением специалистов отдела информационных технологий и пользователей - непосредственных участников инцидента.

3.3. Анализ проводит комиссия, состав которой определяет администратор безопасности.

3.4. Сроки анализа инцидента определяются по категории инцидента. Анализ инцидентов 1, 2, 3 категорий проводят немедленно после возникновения инцидента в целях максимального ускорения устранения последствий инцидента. Анализ инцидентов 4-8 категорий проводят не позднее одного рабочего дня с момента возникновения инцидента.

3.5. Анализ инцидента оформляется Актом расследования инцидента информационной безопасности (приложение к настоящей инструкции).

3.6. Устранение причин и последствий инцидента осуществляет администратор безопасности совместно с администраторами системными по установленным правилам и в установленные сроки.

3.7. Перечень мероприятий, направленных на предотвращение инцидента в будущем формирует, утверждает у руководителя организации и организует выполнение администратор безопасности. Форма перечня мероприятий не регламентируется.

4. ПОРЯДОК РАЗБИРАТЕЛЬСТВА ПО ИНЦИДЕНТУ

4.1. Внутреннее расследование (разбирательство) – деятельность комиссии, направленная на сбор, анализ и оценку информации и документов в целях установления причин и виновных лиц в совершении деяния, повлекшего неблагоприятные последствия для КГБОУ ХКЦВР Созвездие или отдельных работников.

4.2. Внутреннее расследование проводится при получении сведений о фактах нарушения режима конфиденциальности информации, либо о фактах приготовления или попыток к его нарушению.

4.3. Проведение внутреннего расследования осуществляет комиссия, назначаемая администратором безопасности.

4.4. Администратор безопасности организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений, готовит и ведёт заседания комиссии, подписывает протоколы заседаний.

4.5. При проведении внутреннего расследования устанавливаются:

4.5.1. Наличие самого факта совершения деяния, служащего основанием для вынесения соответствующего решения.

4.5.2. Время, место и обстоятельства совершения противоправного деяния, а также оценка его последствий.

4.5.3. Конкретный работник, совершивший установленное деяние.

4.5.4. Наличие и степень вины работника в совершении деяния.

4.5.5. Цели и мотивы совершения деяния, и их оценки, оценки обстоятельств, смягчающих или отягчающих ответственность, в том числе причин и условий, способствовавших совершению данного деяния.

4.6. В целях внутреннего расследования все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

4.7. Работник, совершивший установленное деяние, нарушивший режим защиты информации или делавший попытки (приготовления) к его нарушению, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений комиссией составляется акт.

4.8. Работник имеет право, по согласованию с администратором безопасности, знакомиться с материалами расследования, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании расследования работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

4.9. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением внутреннего расследования, работник обязан сообщить об этом комиссии.

4.10. До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения внутреннего расследования и ставшие известные им обстоятельства.

4.11. В процессе проведения внутреннего расследования комиссией выясняются:

4.11.1. Перечень разглашенных документов и сведений.

4.11.2. Причины разглашения информации.

4.11.3. Лица, виновные в разглашении.

4.11.4. Размер (экспертную оценку) причиненного ущерба.

4.11.5. Недостатки и нарушения, допущенные работниками.

4.11.6. Иные обстоятельства, необходимые для определения причин разглашения информации, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

4.12. По завершении внутреннего расследования комиссией составляется заключение. В заключении указываются:

4.12.1. Основание для проведения внутреннего расследования.

4.12.2. Состав комиссии и время проведения внутреннего расследования.

4.12.3. Сведения о времени, месте и обстоятельствах совершения противоправного деяния.

4.12.4. Сведения о работнике, совершившем противоправное деяние (должность, фамилия, имя, отчество, год рождения, время работы в учреждении, а также в занимаемой должности).

4.12.5. Мотивы и цели совершения работником противоправного деяния.

4.12.6. Причины и условия совершения деяния.

4.12.7. Данные о характере и размерах причиненного в результате противоправного деяния ущерба, причинную связь деяния и причиненного ущерба.

4.12.8. Предложения о мере ответственности работника, совершившего противоправное деяние.

4.13. На основании заключения выносится решение о применении мер ответственности к работнику, виновному в разглашении информации, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

4.14. Все материалы внутренних расследований хранятся в течение 5 лет. Копии заключения и распоряжения по результатам внутреннего расследования приобщаются к личному делу работника, в отношении которого оно проводилось.

5. ПОРЯДОК УСТРАНЕНИЯ ПОСЛЕДСТВИЙ ИНЦИДЕНТА

5.1. Ответственным лицом за устранение последствий инцидента является администратор безопасности. При устранении последствий инцидента администратор безопасности вправе привлекать к работам по устранению инцидента других сотрудников.

5.2. При нарушении конфиденциальности информации, обрабатываемой в ИС или подозрении в ее нарушении администратор безопасности:

5.2.1. Проводит процедуру смены паролей пользователям.

5.2.2. Пересматривает и обновляет, с учетом содержания инцидента, матрицу доступа к ресурсам.

5.3. При нарушении целостности и доступности информации администратор безопасности:

5.3.1. Организует переустановку программного обеспечения и системы защиты информации с дистрибутивных носителей используемого программного обеспечения.

5.3.2. Организует переустановку обрабатываемой информации с резервных копий.

5.3.3. Проверяет конфигурацию и систему защиты информации.

6. ПОРЯДОК УСТРАНЕНИЯ ПРИЧИН ИНЦИДЕНТА

6.1. Причины инцидентов разделяют на аппаратно-программные и организационные.

6.2. К аппаратно – программным причинам относятся все причины, связанные с недостатками аппаратной, программной части и системы защиты информации (ошибки кода, ошибки настроек, неисправности оборудования, электромагнитная совместимость и т.п.).

6.3. К организационным причинам относятся недостатки организационно-распорядительной документации, ошибки пользователей, недостатки физической защиты доступа и т.п.

6.4. Устранение причин инцидентов осуществляет администратор безопасности. Сроки и состав действий определяются индивидуально по каждому инциденту.

7. НОРМАТИВНЫЕ И ПРАВОВЫЕ ДОКУМЕНТЫ

7.1. Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

7.2. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Приложение
к Инструкции по управлению
инцидентами

Министерство образования и науки
Хабаровского края
Краевое государственное
бюджетное образовательное учреждение
«ХАБАРОВСКИЙ КРАЕВОЙ ДЕТСКИЙ
ЦЕНТР ВНЕШКОЛЬНОЙ РАБОТЫ
«СОЗВЕЗДИЕ»
(КГБОУ ХКЦВР Созвездие)

АКТ

_____ № _____

г. Хабаровск

расследования инцидента
информационной безопасности

Место проведение проверки: _____

Комиссия в составе:

Председатель

_____(Ф.И.О.)

Члены комиссии:

_____(Ф.И.О.)

_____(Ф.И.О.)

Провела расследование инцидента информационной безопасности:

_____

_____

_____

_____

В ходе расследования выявлены нанесенный организации ущерб:

_____

_____

_____

_____

и причины инцидента:

_____

_____

_____

Заключения и выводы комиссии: _____

_____

Предписания:

_____

_____

_____

_____

Председатель комиссии _____ _____
(подпись) (расшифровка подписи)

Члены комиссии: _____ _____
(подпись) (расшифровка подписи)

_____ _____
(подпись) (расшифровка подписи)