бюджетное профессиональное образовательное учреждение Вологодской области «Великоустюгский многопрофильный колледж»

УТВЕРЖДЕНЫ
приказом директора колледжа
от 24.05.2022 г. № 236

ПРАВИЛА

«24» 05 2022 г. № 17

г. Великий Устюг

управления инцидентами информационной безопасности

1. Общие положения

1.1. Инциденты информационной безопасности информационной системы (далее ИС) разделены на категории:

1.1.1. Категория 1 - отказ технических средств ИС и средств защиты информации (далее СЗИ) (отказ в обслуживании сервисов, средств обработки информации, оборудования).

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

1.1.3. Категория 3 - сбои программного обеспечения ИС и СЗИ.

1.1.4. Категория 4 - неконтролируемые изменения конфигурации ИС и СЗИ.

1.1.5. Категория 5 - нарушение физических мер защиты информации ИС.

1.1.6. Категория 6 - нарушение правил доступа к информации, содержащейся в ИС.

1.1.7. Категория 7 - несоблюдение пользователями ИС требований ОРД по защите информации.

1.1.8. Категория 8 - ошибки пользователей ИС.

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

2. Порядок выявления инцидентов

2.1. Выявление и учет инцидентов организует инженер учреждения на основе сообщений пользователей и анализа событий информационной безопасности.

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

2.3. При выявлении инцидента осуществляют оповещение пользователей ИС об инциденте. Форму и порядок оповещения устанавливает инженер учреждения.

3. Порядок реагирования на инциденты

3.1. При реагировании на инциденты:

3.1.1. Инженер осуществляет анализ инцидента:

- проводит оценку нанесенного материального ущерба;
- выявляет неучтенные в системе защиты информации угрозы безопасности;
- расследует причины возникновения инцидента.

3.1.2. Устраняет причины и последствия инцидента.

3.1.3. Формирует перечень мероприятий по недопущению инцидента в будущем.

3.2. Анализ инцидента организует инженер с привлечением программиста и пользователей - непосредственных участников инцидента.

3.3. Анализ проводит комиссия, состав которой определяет директор учреждения.

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 1 рабочего дня с момента возникновения инцидента.

3.5. Анализ инцидента оформляется актом расследования инцидента информационной безопасности (*Приложение 1*).

3.6. Устранение причин и последствий инцидента осуществляет инженер совместно с системным администратором по установленным правилам и в установленные сроки.

3.7. Системный администратор формирует и утверждает у директора учреждения Перечень мероприятий, направленных на недопущение инцидента в будущем, а также организует их выполнение. 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 учреждения, его структурных подразделений или отдельных работников.

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

4.3. Проведение внутреннего расследования осуществляет комиссия, назначаемая директором учреждения.

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

4.5. При проведении внутреннего расследования устанавливаются:

- наличие самого факта совершения деяния, служащего основанием для вынесения соответствующего решения;
- время, место и обстоятельства совершения противоправного деяния, а также оценка его последствий;
- конкретный работник, совершивший установленное деяние;
- наличие и степень вины работника в совершении деяния;
- 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 учреждения 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 директором учреждения, 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 председателю 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:

- перечень разглашенных документов и сведений, составляющих конфиденциальную информацию;
- причины разглашения конфиденциальной информации;
- лица, виновные в разглашении;
- размер (экспертную оценку) причиненного ущерба;

- недостатки и нарушения, допущенные работниками при работе с конфиденциальной информацией;
- иные обстоятельства, необходимые для определения причин разглашения конфиденциальной информации, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

4.12. По завершении внутреннего расследования комиссией составляется заключение.

В заключении указываются:
- основание для проведения внутреннего расследования;
- состав комиссии и время проведения внутреннего расследования;
- сведения о времени, месте и обстоятельствах совершения противоправного деяния;
- сведения о работнике, совершившем противоправное деяние (должность, фамилия, имя, отчество, год рождения, время работы в учреждении, а также в занимаемой должности);
- мотивы и цели совершения работником противоправного деяния;
- причины и условия совершения деяния;
- данные о характере и размерах причиненного в результате противоправного деяния ущерба, причинную связь деяния и причиненного ущерба;
- предложения о мере ответственности работника, совершившего противоправное деяние.

4.13. На основании заключения выносится решение о применении мер ответственности к работнику, виновному в разглашении конфиденциальной 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 относятся к конфиденциальным сведениям и 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 в учреждении является системный администратор. При устранении последствий инцидента системный администратор вправе привлекать к работам по устранению инцидента инженеров, программиста.

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

- проводит процедуру смены паролей пользователям;
- пересматривает и обновляет, с учетом содержания инцидента, матрицу доступа к ресурсам ИС.

При нарушении целостности и доступности информации инженер:

- организует переустановку программного обеспечения ИС и системы защиты информации с дистрибутивных носителей используемого программного обеспечения;

- организует переустановку обрабатываемой информации с резервных копий;

- проверяет конфигурацию ИС и ее системы защиты информации (при необходимости восстанавливает конфигурацию в соответствии с эксплуатационной документацией).

6. Порядок устранения причин инцидента

6.1. Причины инцидентов в ИС разделяют на следующие типы:

- аппаратно – программные причины;

- организационные причины.

6.2. К аппаратно – программным причинам относятся все причины, связанные с недостатками аппаратной и программной частей ИС и ее 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, дисциплинарные, злой умысел и т.п.

6.4. Устранение аппаратно – программных причин инцидентов осуществляет инженер. Сроки и состав действий определяются индивидуально по каждому инциденту.

6.5. Устранение организационных причин осуществляет инженер совместно с программистом. Сроки и состав действий устанавливаются индивидуально по каждому инциденту.

7. Заключительные положения

7.1. Системный администратор, инженеры и программист должны быть:

- ознакомлены с настоящими Правилами до начала работы с ИС под подпись;

- предупреждены об ответственности за действия, нарушающие требования настоящих Правил.

7.2. Сотрудники учреждения несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами, в пределах, определенных действующим законодательством Российской Федерации.

8. Нормативные и правовые документы

8.1. Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

8.2. Приказ ФСТЭК России от 23.03.2017 года № 49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21, и в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31».

8.3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Рассмотрено
Советом Учреждения
Протокол № 22
«24» 05 2022 г.

В дело № 01-14
«24» 05 2022 г.

УТВЕРЖДАЮ
Директор БПОУ ВО «ВУМК»
_____Ф.И.О.
« _____ » _____ 20____ г.

АКТ № _____
расследования инцидента информационной безопасности

г. _____ « ___ » _____ 20___ г.

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)
Члены комиссии _____ (подпись)
_____ (подпись)