МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ САМАРСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
«ТОЛЬЯТТИНСКИЙ ХИМИКО-ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

УТВЕРЖДАЮ
и. о. директора ГБПОУ «Тольяттинский химико-технологический техникум»
_____ Т. А. Михайленко
Приказ от «23» января 2019 г. № 6/1-од

Инструкция
по работе с инцидентами в информационных системах ГБПОУ «Тольяттинский химико-технологический техникум»

СОГЛАСОВАНО
Советом Учреждения
протокол от 22.01.2019 г. № 1

1. Общие положения

1.2.. Инструкция по работе с инцидентами информационной безопасности (далее - Инструкция) регламентирует порядок работы с инцидентами информационной безопасности в ГБПОУ «Тольяттинский химико-технологический техникум» (далее — Учреждение).
1.2. Правила, устанавливаемые положениями настоящей Инструкции обязательны для исполнения всеми сотрудниками Учреждения.
1.3. Ответственность за выявление инцидентов информационной безопасности и реагирование на них в Учреждении возлагается на администратора безопасности информационных систем.

2. Порядок работы с инцидентрами информационной безопасности

2.1 Администратор безопасности информационных систем имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед руководителем Учреждения) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.
2.2. Администратор безопасности информационных систем обязан:
1) вести журнал учета нештатных ситуаций, выполнения профилактических и ремонтных работ в ГБПОУ «Тольяттинский химико-технологический техникум», установки и модификации аппаратных и программных средств информационных систем. Нештатная ситуация это событие, действие повлекшее за собой риски безопасности защищаемой информации и создающие предпосылки к нарушению критериев безопасности информации. Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои программного обеспечения, стихийные бедствия и т.п.).
В журнале описывается инцидент с указанием следующих данных:
- дата и время;
- причина (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описание инцидента и задействованных лиц;
- информация о последствиях (экономические убытки (в связи с заменой СЗИ, переаттестации; трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам персональных данных, юридические последствия для Учреждения и т.п.) и о времени устранения инцидента.
Журнал учета с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению возникновения повторного инцидента (рецидива).
2) При получении информации о фактах нарушения политики и правил безопасности, а также попыток использования внешними нарушителями атак, в

том числе с использованием методов социальной инженерии - немедленно докладывать ответственному за организацию обработки персональных данных, инициировать проведение служебной проверки (при нарушениях со стороны ответственного за организацию обработки персональных данных докладывать необходимо руководителю Учреждения), зарегистрировать инцидент в журнале учёта.

3) Осуществлять регулярный (не реже двух раз в месяц) просмотр журнала учета на предмет выявления инцидентов информационной безопасности и реагирование на них в случае необходимости.

4) Реагировать на поступление в ИС спама (в случае присутствия данной информации в журналах событий межсетевого экрана) путем блокирования атакующего хоста.

2.3 Каждый сотрудник Учреждения обязан:

1) При получении информации о фактах нарушения политики и правил безопасности, а также попыток использования внешними нарушителями атак, в том числе с использованием методов социальной инженерии немедленно докладывать администратору безопасности информационных систем (при нарушениях со стороны администратора безопасности информационных систем докладывать необходимо ответственному за организацию обработки персональных данных либо руководителю Учреждения).

2) Согласовывать следующие действия с администратором безопасности информационных систем:

- замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
- установка дополнительного ПО;
- изменение сетевых настроек рабочего места;
- замена, изменение любой аппаратной части рабочего места.

2.4. В случае возникновения рецидива со стороны пользователя или администратора безопасности информационных систем, по ходатайству ответственного за организацию обработки персональных данных, руководителем Учреждения накладывается дисциплинарное взыскание.

2.5. Сокрытие нарушений и инцидентов информационной безопасности, вызванных любыми должностными лицами Учреждения, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов информационной безопасности, вызванных действиями администратора безопасности информационных систем и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта, должно наказываться.

2.6. Ответственный за организацию обработки персональных данных не может требовать от администратора безопасности информационных систем действий, направленных на нарушение настоящей Инструкции и других организационно-распорядительных документов Учреждения, требовать сокрытия инцидентов информационной безопасности, вызванных любыми должностными лицами, требовать сообщения ему паролей доступа (к средствам защиты информации).

Приложение

ЖУРНАЛ
учета нештатных ситуаций, выполнения профилактических и ремонтных работ

№№ п/п	Дата и время	Описание инцидента	Причина инцидента	Информация о последствиях	Дата и время устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
учета выявленных инцидентов информационной безопасности

№№ п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата и время устранения инцидента	Подпись ответственного лица	Примечание