П-109/2019

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

Протокол заседания Совета Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета обучающихся
Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета родителей
Учреждения
от 29.10.2019г. № 20

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»
_____А.Н. Сакеев
«29» октября 2019г.

Приказ № 522 о/д от 29.10.2019

**Инструкция**
**пользователя по обеспечению безопасности сведений конфиденциального характера и персональные данные, при возникновении внештатных ситуаций**

## 1. Общие положения

1.1. Настоящая инструкция определяет действия работников ГБПОУ «ТК им. Н.Д. Кузнецова» (далее – Учреждение) в случае возникновения нештатных ситуаций в процессах обработки сведений конфиденциального характера и персональных данных в информационной системе.

1.2. Положения инструкции обязательны для исполнения всеми должностными лицами Учреждения в части выполнения вмененных им обязанностей.

1.3. Общими требованиями ко всем работникам Учреждения, в случае возникновения нештатной ситуации являются:

- работник, обнаруживший нештатную ситуацию, немедленно ставит в известность своего непосредственного руководителя и Администратора безопасности информации;
- Администратор безопасности информации обязан проводить анализ ситуации и, в случае невозможности исправить положение, ставит в известность руководителя Учреждения.
- Кроме этого, Администратор безопасности информации для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей информационной системы Уреждения, а также Администратора информационной системы;
- по факту возникновения нештатной ситуации и выяснению причин ее проявления проводится служебное расследование.

## 2. Действия пользователей информационной системы при возникновении нештатных ситуаций

2.1. Сбой программного обеспечения.

2.1.1. Администратор безопасности информации совместно с Администратором информационной системы выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультации с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а так же файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте Администратор безопасности информации сообщает руководителю Учреждения для принятия решения.

2.2. Отключение электропитания технических средств информационной системы.

2.2.1. Администратор безопасности информации совместно с Администратором информационной системы проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте Администратор безопасности информации сообщает руководителю Учреждения для принятия решения.

2.3. Выход из строя технических средств информационной системы.

2.3.1. Администратор информационной системы совместно с Администратором безопасности информации выполняют мероприятия по немедленному вводу в действие резервной рабочей станции для обеспечения непрерывной работы информационной системы.

2.3.2. О выходе из строя рабочей станции Администратор информационной системы, ответственный за эксплуатацию рабочей станции, сообщает руководителю Учреждения.

2.3.3. При необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте Администратор безопасности информации сообщает руководителю Учреждения для принятия решения.

2.4. Потеря данных.

2.4.1. При обнаружении потери данных Администратор информационной системы проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность программного обеспечения, целостность и работоспособность оборудования).

2.4.2. При необходимости Администратором информационной системы производится восстановление программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте Администратор информационной системы сообщает Администратору безопасности информации. Администратор безопасности информации сообщает руководителю Учреждения для принятия решения.

2.5. Обнаружение вредоносной программы в программной среде средств автоматизации информационной системы.

2.5.1. При обнаружении вредоносной программы (ВП) производится её локализация с целью предотвращения её дальнейшего распространения. Администратором информационной системы и Администратором безопасности информации проводится анализ состояния рабочей станции.

2.5.2. В результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки рабочей станции данные могут быть потеряны. После успешной ликвидации ВП сохранённые данные подвергаются повторной проверке на наличие ВП. Кроме того, при обнаружении ВП следует руководствоваться инструкцией по эксплуатации применяемого антивирусного программного обеспечения.

2.5.3. После ликвидации ВП, проводится внеочередная проверка на всех средствах информационной системы и машинных носителях информации, с применением обновлённых антивирусных баз. При необходимости производится восстановление программного обеспечения и данных из резервных копий с составлением акта.

2.5.4. По факту появления ВП в локальной вычислительной сети проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем Учреждения.

2.6. Утечка информации.

2.6.1. При обнаружении утечки информации ставится в известность Администратор безопасности информации и начальник структурного подразделения. По факту

инициируется процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищённости процессов информационной системы и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

2.7. Взлом операционной системы средств автоматизации информационной системы (несанкционированное получение доступа к ресурсам операционной системы).

2.7.1. При обнаружении взлома рабочей станции ставится в известность руководитель Учреждения.

2.7.2. По возможности производится временное отключение рабочей станции. Возможен временный переход на резервную рабочую станцию.

2.7.3. Администратором информационной системы проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения. Администратором информационной системы проводится анализ состояния файлов - скриптов и журналов, производится смена всех паролей, которые имели отношение к данной рабочей станции.

2.7.4. В случае необходимости Администратором информационной системы производится восстановление программного обеспечения и восстановление данных из эталонного архива и резервных копий с составлением акта.

2.7.5. По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в рабочую станцию.

2.8. Попытка несанкционированного доступа (НСД).

2.8.1. При попытке НСД, Администратором информационной системы и Администратором безопасности информации проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

2.8.2. Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, Администратором информационной системы устанавливаются такие обновления.

2.8.3. По факту попытки НСД проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем Учреждения.

2.8.4. В случае установления в ходе служебного расследования факта, осуществления попытки НСД со стороны внешних по отношению к информационной системе субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

2.9. Компрометация ключевой информации (паролей доступа).

2.9.1. При компрометации ключевой информации (пароля доступа) Администратором безопасности информации проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесённого) ущерба.

2.9.2. О произошедшем инциденте Администратор безопасности информации сообщает руководителю Учреждения для принятия решения.

2.10. Физическое повреждение или хищение оборудования технических средств информационной системы.

2.10.1. Работником, обнаружившим физическое повреждение элементов информационной системы, ставится в известность: непосредственный руководитель, Администратор безопасности информации и Администратор информационной системы.

2.10.2. Администратором информационной системы совместно с Администратором безопасности информации проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов информационной системы и возможные угрозы информационной безопасности.

2.10.3. О факте повреждения элементов информационной системы Администратор безопасности информации докладывает руководителю Организации.

2.10.4. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование.

2.10.5. Администратором информационной системы проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.10.6. При необходимости Администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта

2.11. Невыполнение установленных правил информационной безопасности (правил работы в информационной системе), использование информационной системы с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

2.11.1. Работником, обнаружившим невыполнение установленных правил информационной безопасности, использование информационной системы с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставится в известность: непосредственный руководитель и Администратор безопасности информации.

2.11.2. Администратором безопасности информации проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.11.3. Об обнаруженном факте Администратор безопасности информации докладывает руководителю Учреждения.

2.11.4. При необходимости по решению руководителя Учреждения по фактам выявленных нарушений проводится служебное расследование.

2.12. Ошибки пользователей.

2.12.1. В случае возникновения сбоя, связанного с ошибками пользователей, руководитель структурного подразделения Организации, в котором произошёл инцидент, ставит в известность Администратора безопасности информации и Администратора информационной системы.

2.12.2. Администратором безопасности информации совместно с Администратором

2.12.3. информационной системы проводятся анализ с целью оценки возможности утечки или повреждения информации.

2.12.4. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения и данных.

2.12.5. При необходимости Администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.12.6. В случае нанесения Учреждению значительного ущерба вследствие ошибок пользователей, проводится служебное расследование.

2.13. Отказ в обслуживании.

2.13.1. Пользователем, обнаружившим отказ в обслуживании, ставится в известность; непосредственный руководитель, Администратор безопасности информации и Администратор информационной системы.

2.13.2. Администратором информационной системы и Администратором безопасности информации проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.13.3. Администратором информационной системы проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.13.4. При необходимости, Администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.13.5. О причинах инцидента и принятых мерах Администратор информационной системы информирует Администратора безопасности информации и руководителя Учреждения.

2.14. Несанкционированные изменения состава программных и аппаратных средств (конфигурации) информационной системы.

2.14.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) информационной системы Администратором безопасности информации проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.14.2. Администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта, а также (при необходимости) проверка на наличие компьютерных ВП.

2.14.3. Об инциденте Администратор безопасности информации докладывает руководителю Учреждения.

2.15. Техногенные и природные проявления нештатных ситуаций.

2.15.1. При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), работнику, обнаружившему факт возникновения нештатной ситуации:

- немедленно оповестить других работников и принять все меры для самостоятельной оперативной защиты помещения;
- немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);
- немедленно сообщить своему непосредственному руководителю и Администратору безопасности информации.

2.15.2. После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.

2.15.1. Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

Разработчик:
заместитель директора по общим вопросам

_____/ Ю.Ю. Алексеев /

**Лист**
**ознакомления с «Инструкцией пользователя по обеспечению безопасности сведений конфиденциального характера и персональные данные, при возникновении внештатных ситуаций»**

| № п/п | ФИО | Должность | Подпись, дата |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |