Подписано цифровой подписью: Пальчук М.И.
DN: cn=Пальчук М.И., o=ГБПОУ РК "Романовский колледж индустрии гостеприимства", ou=Директор, email=043@crimeaedu.ru, c=RU
Дата: 2023.05.11 11:08:54 +03'00'

УТВЕРЖДАЮ
Директор
ГБПОУ РК «РКИГ»
_____ Пальчук М. И.
Приказ № 37 от 09.03.2023 г.

Инструкция о действиях лиц, допущенных к работе в информационной системе персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ, в случае возникновения нештатных ситуаций

1 Общие положения

1.1 Настоящая инструкция определяет действия лиц, допущенных к работе в информационной системе персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ (далее - ИСПДн ОИ ФЦТ) в случае возникновения инцидентов в процессах обработки персональных данных.

1.2 Положения настоящей Инструкции обязательны для исполнения всеми должностными лицами, допущенными к работе в ИСПДн ОИ ФЦТ в части выполнения возложенных на них обязанностей.

1.3 . Общими требованиями ко всем лицам, допущенным к работе в ИСПДн ОИ ФЦТ, в случае возникновения нештатной ситуации или другого инцидента являются:

- лицо, обнаружившее нештатную ситуацию или другой инцидент, немедленно ставит в известность Администратора (сетевого или безопасности) ИСПДн ОИ ФЦТ;
- Администратор (сетевой или безопасности) обязан провести анализ ситуации и, в случае невозможности исправить положение, поставить в известность руководство Учреждения. Кроме этого, Администратор ИСПДн ОИ ФЦТ для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей ИСПДн ОИ ФЦТ;
- по факту возникновения инцидента и выяснению причин его проявления по решению руководства может быть назначена комиссия по реагированию на инциденты ИБ и проведено служебное расследование.

2 Действия пользователей ИСПДн ОИ ФЦТ при возникновении нештатных ситуаций

2.1 Сбой программного обеспечения.

2.1.1 Администратор ИСПДн ОИ ФЦТ выясняет причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте Администратор ИСПДн ОИ ФЦТ сообщает руководителю Учреждения для принятия решения по существу.

2.2 Отключение электропитания технических средств ИСПДн ОИ ФЦТ.

2.2.1 Администратор ИСПДн ОИ ФЦТ проводит 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 ИСПДн ОИ ФЦТ сообщает руководителю Учреждения для принятия решения по существу.

2.3 Выход из строя технических средств ИСПДн ОИ ФЦТ (рабочих станций, источников бесперебойного питания, программно-аппаратных средств межсетевого экранирования и т.д.).

2.3.1 Администратор ИСПДн ОИ ФЦТ совместно с Администратором безопасности ИСПДн ОИ ФЦТ выполняют мероприятия по ремонту неисправного технического средства ИСПДн ОИ ФЦТ.

2.3.2 В случае необходимости уведомить о выходе из строя технических средств ИСПДн ОИ ФЦТ администратора ИСПДн ОИ ФЦТ.

2.3.3 При необходимости производятся работы по восстановлению программного обеспечения из эталонных копий с составлением акта. О произошедшем инциденте необходимо сообщить администратору безопасности для принятия решения по существу.

2.4 Обнаружение вредоносной программы в программной среде ИСПДн ОИ ФЦТ.

2.4.1 При обнаружении вредоносной программы (ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженную рабочую станцию рекомендуется физически отсоединить от локальной вычислительной сети, и Администратор безопасности ИСПДн ОИ ФЦТ проводит анализ состояния рабочей станции.

2.4.2 После ликвидации ВП проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения из эталонных копий с составлением акта.

2.4.3 По факту появления ВП в локальной вычислительной сети может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем.

2.5 Утечка информации.

2.5.1 При обнаружении утечки информации ставится в известность Администратор безопасности ИСПДн ОИ ФЦТ. По факту может быть произведена процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИСПДн ОИ ФЦТ и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

2.6 Взлом операционной системы ИСПДн ОИ ФЦТ (несанкционированное получение доступа к ресурсам операционной системы).

2.6.1 При обнаружении взлома рабочей станции ставятся в известность Администратор ИСПДн ОИ ФЦТ и Администратор безопасности ИСПДн ОИ ФЦТ.

2.6.2 По возможности производится временное отключение рабочей станции от локальной вычислительной сети ИСПДн ОИ ФЦТ для проверки на наличие ВП.

2.6.3 Администратором безопасности ИСПДн ОИ ФЦТ проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, проводится анализ состояния файлов - скриптов и

журналов сервера, производится смена всех паролей, которые имели отношение к данному серверу.

2.6.4 В случае необходимости производится восстановление программного обеспечения из эталонных копий с составлением акта.

2.6.5 По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в ИСПДн ОИ ФЦТ, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах ИСПДн ОИ ФЦТ.

2.7 Попытка несанкционированного доступа (НСД).

2.7.1 . При попытке НСД Администратором безопасности ИСПДн ОИ ФЦТ 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.

2.7.2 Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, Администратором ИСПДн ОИ ФЦТ устанавливаются такие обновления.

2.7.3 По факту попытки НСД может быть проведено служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем Учреждения.

2.7.4 В случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению к ИСПДн ОИ ФЦТ 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.

2.8 Компрометация ключевой информации (паролей доступа).

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

2.8.2 О произошедшем инциденте сообщается руководителю Учреждения для принятия решения по существу.

2.9 Физическое повреждение или хищение оборудования технических средств ИСПДн ОИ ФЦТ.

2.9.1 Сотрудником, обнаружившим физическое повреждение элементов ИСПДн ОИ ФЦТ, ставятся в известность: Администратор ИСПДн ОИ ФЦТ, Администратор безопасности ИСПДн ОИ ФЦТ.

2.9.2 Администратором безопасности ИСПДн ОИ ФЦТ проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн ОИ ФЦТ и возможные угрозы информационной безопасности.

2.9.3 О факте повреждения элементов ИСПДн ОИ ФЦТ в случае необходимости Администратор безопасности ИСПДн ОИ ФЦТ докладывает руководителю Учреждения.

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

2.9.5 Администратором безопасности ИСПДн ОИ ФЦТ проводится проверка

программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.9.6 При необходимости Администратором ИСПДн ОИ ФЦТ проводятся мероприятия по восстановлению программного обеспечения из эталонных копий с составлением акта.

2.10 Невыполнение установленных правил ИБ (правил работы ИСПДн ОИ ФЦТ), использование ИСПДн ОИ ФЦТ с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

2.10.1 Сотрудником, обнаружившим невыполнение установленных правил ИБ, использование ИСПДн ОИ ФЦТ с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставятся в известность Администратор безопасности ИСПДн ОИ ФЦТ.

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

2.10.3 Об обнаруженном факте Администратор безопасности ИСПДн ОИ ФЦТ в случае необходимости докладывает руководителю Учреждения.

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

2.11 Ошибки сотрудников.

2.11.1 В случае возникновения сбоя, связанного с ошибками сотрудников, Администратором безопасности ИСПДн ОИ ФЦТ проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения.

2.11.2 При необходимости проводятся мероприятия по восстановлению программного обеспечения и данных из эталонных копий с составлением акта.

2.11.3 В случае нанесения значительного ущерба вследствие ошибок работников по решению руководства Учреждения может быть проведено служебное расследование.

2.12 Отказ в обслуживании.

2.12.1 Сотрудником, обнаружившим отказ в обслуживании, ставятся в известность Администратор безопасности ИСПДн ОИ ФЦТ.

2.12.2 . Администратором безопасности ИСПДн ОИ ФЦТ проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.12.3 Администратором безопасности ИСПДн ОИ ФЦТ проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.12.4 При необходимости, проводятся мероприятия по восстановлению программного обеспечения с составлением акта.

2.12.5 О причинах инцидента и принятых мерах Администратор безопасности ИСПДн ОИ ФЦТ в случае необходимости информирует руководителя Учреждения.

2.13 Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн ОИ ФЦТ.

2.13.1 В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИСПДн ОИ ФЦТ Администратором безопасности ИСПДн ОИ ФЦТ проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются

возможные угрозы ИБ в результате инцидента.

2.13.2 Администратором ИСПДн ОИ ФЦТ совместно с Администратором безопасности ИСПДн ОИ ФЦТ проводятся мероприятия по восстановлению программного обеспечения, а также (при необходимости) проверка на наличие компьютерных ВП.

2.13.3 Об инциденте необходимо доложить руководителю Учреждения.

2.14 Техногенные и природные проявления нештатных ситуаций.

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

- немедленно оповестить других сотрудников 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 Администратору ИСПДн ОИ ФЦТ и Администратору безопасности.

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

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

Ведущий специалист по защите информации А. О. Грибенников