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 11:14:15 +03'00'

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

Инструкция
администратора безопасности
информационной системы персональных данных
обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ

1 Общее положения

1.1 Настоящая Инструкция определяет обязанности Администратора безопасности информационной системы персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ (далее - ИСПДн ОИ ФЦТ).

1.2 Администратор безопасности в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России, ФСБ России, регламентирующими документами Учреждения и другими документами.

1.3 Администратор безопасности назначается руководителем Учреждения.

1.4 Администратор безопасности по вопросам обеспечения безопасности информации подчиняется руководителю Учреждения.

1.5 Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое).

1.6 Администратор безопасности осуществляет методическое руководство пользователями ИСПДн ОИ ФЦТ в вопросах обеспечения правильной работы с используемыми в ИСПДн ОИ ФЦТ средствами защиты информации (далее - СЗИ).

1.7 Требования Администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн ОИ ФЦТ.

1.8 Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн ОИ ФЦТ, состояние и поддержание установленного уровня защиты ИСПДн ОИ ФЦТ.

2 Задачи администратора безопасности

2.1 Основными задачами Администратора безопасности являются:

- поддержание необходимого уровня защиты ИСПДн ОИ ФЦТ от несанкционированного доступа (НСД) к информации, в т.н. ПДн;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации, в т. ч. ПДн;
- установка средств защиты информации и контроль выполнения правил их эксплуатации;
- сопровождение средств защиты информации (СЗИ) от НСД и основных технических средств и систем (ОТСС) ИСПДн ОИ ФЦТ;
- периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов ИБ;
- оперативное реагирование на нарушения требований по ИБ в ИСПДн ОИ ФЦТ и участие в их прекращении.

2.2 В рамках выполнения основных задач Администратор безопасности осуществляет:

текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;
- текущий контроль технологического процесса автоматизированной обработки ПДн;
- участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности ПДн;
- контроль соблюдения нормативных требований по защите ПДн, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации пользователями ИСПДн ОИ ФЦТ;
- методическую помощь пользователям ИСПДн ОИ ФЦТ по вопросам обеспечения безопасности ПДн и работы с используемыми СЗИ.

3 Обязанности администратора безопасности информации

Администратор безопасности обязан:

3.1 Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИСПДн ОИ ФЦТ.

3.2 Участвовать в установке, настройке и сопровождении СЗИ, используемых в ИСПДн ОИ ФЦТ.

3.3 Участвовать в приемке новых программных средств обработки информации.

3.4 Обеспечить доступ к защищаемой информации пользователям ИСПДн ОИ ФЦТ согласно их правам доступа.

3.5 Уточнять в установленном порядке обязанности пользователей ИСПДн ОИ ФЦТ при обработке ПДн.

3.6 Вести контроль осуществления резервного копирования информации.

3.7 Анализировать состояние защиты ИСПДн ОИ ФЦТ.

3.8 Контролировать правильность функционирования средств защиты информации и неизменность их настроек.

3.9 Контролировать физическую сохранность технических средств обработки информации.

3.10 Контролировать исполнение пользователями ИСПДн ОИ ФЦТ

введенного режима безопасности, а также правильность работы с элементами ИСПДн ОИ ФЦТ и средствами защиты информации.

3.11 Контролировать исполнение пользователями правил парольной политики.

3.12 Еженедельно анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

3.13 Не допускать установку, использование, хранение и размножение в ИСПДн ОИ ФЦТ программных средств, не связанных с выполнением функциональных задач.

3.14 Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) пользователей ИСПДн ОИ ФЦТ.

3.15 Оказывать помощь пользователям ИСПДн ОИ ФЦТ в части применения средств защиты и консультировать по вопросам введенного режима защиты.

3.16 Информировать руководство о состоянии защиты ИСПДн ОИ ФЦТ и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.17 В случае отказа работоспособности СЗИ ИСПДн ОИ ФЦТ принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.18 В случае выявления нарушений режима безопасности ПДн, а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

3.19 В случае изменения используемых информационных технологий, состава и размещения средств и систем информатики, условий их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в «Аттестате соответствия») произвести извещение органа по аттестации, выдавшего «Аттестат соответствия».

4 Права администратора безопасности

Администратор безопасности имеет право:

4.1 Отключать от ресурсов ИСПДн ОИ ФЦТ пользователей, осуществивших НСД к защищаемым ресурсам ИСПДн ОИ ФЦТ или нарушивших другие требования по ИБ.

4.2 Давать пользователям обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.3 Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИСПДн ОИ ФЦТ.

4.4 Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн ОИ ФЦТ при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.5 Осуществлять взаимодействие с руководством и персоналом ИСПДн ОИ

ФЦТ по вопросам обеспечения ИБ.

4.6 Запрещать устанавливать на автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

4.7 Запрашивать и получать от пользователей системы информацию и материалы, необходимые для организации своей работы.

4.8 Вносить на рассмотрение руководства предложения по улучшению состояния безопасности ПДн, обрабатываемых на ИСПДн ОИ ФЦТ.

4.9 Принимать участие в проведении мероприятий по контролю за обеспечением безопасности персональных данных.

4.10 Вносить изменения в конфигурацию ИСПДн ОИ ФЦТ и предварительно произведя анализ потенциального воздействия планируемых изменений, согласовав внесение планируемых изменений с должностным лицом (работником), ответственным за обеспечение безопасности ПДн и получив разрешение органа по аттестации, выдавшего «Аттестат соответствия» на ИСПДн ОИ ФЦТ.

5 Действия администратора безопасности при обнаружении попыток НСД

5.1 К попыткам НСД относятся:

- сеансы работы с телекоммуникационными ресурсами ИСПДн ОИ ФЦТ незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий, которых истек, либо в состав полномочий, которых не входят операции доступа к определенным данным или манипулирования ими;

- действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ИСПДн ОИ ФЦТ с использованием учетной записи администратора или другого пользователя ИСПДн ОИ ФЦТ, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

5.2 При выявлении факта/попытки НСД Администратор безопасности обязан:

- прекратить доступ к информационным ресурсам со стороны выявленного участка НСД;

- доложить руководителю Учреждения о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

- известить начальника структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

- проанализировать характер НСД;

- по решению руководства осуществить действия по выяснению причин, приведших к НСД;

- предпринять меры по предотвращению подобных инцидентов в дальнейшем.

6 Ответственность администратора безопасности

6.1 Администраторы безопасности, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального законодательства РФ и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Ведущий специалист по защите информации А. О. Грибенников