Муниципальное автономное учреждение города Новосибирска
«Новосибирский Центр Высшего Спортивного Мастерства»

П Р И К А З

От 18.03.2020 № 01-02-27

Об утверждении инструкций и
ознакомлении с ними
ответственных лиц

С целью организации работ по обеспечению безопасности персональных данных в МАУ «НЦВСМ» и в соответствии с требованиями статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Инструкцию ответственному за организацию обработки и защиты персональных данных (Приложение 1).
2. Утвердить и ввести в действие Инструкцию администратора безопасности информационных систем МАУ «НЦВСМ» (Приложение 2).
3. Утвердить и ввести в действие Инструкцию ответственному за защиту информации, в том числе за обеспечение безопасности персональных данных в информационных системах МАУ «НЦВСМ» (Приложение 3).
4. Утвердить и ввести в действие Инструкцию по работе пользователей в информационных системах МАУ «НЦВСМ» (Приложение 4).
5. Утвердить и ввести в действие Инструкцию о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации, в информационных системах МАУ «НЦВСМ» (Приложение 5).
6. Утвердить и ввести в действие Инструкцию по организации антивирусной защиты в информационных системах персональных данных МАУ «НЦВСМ» (Приложение 6).
7. Утвердить и ввести в действие Инструкцию по организации криптографической защиты в информационных системах персональных данных МАУ «НЦВСМ» (Приложение 7).
8. Утвердить и ввести в действие Инструкцию по организации парольной защиты в информационных системах персональных данных МАУ «НЦВСМ» (Приложение 8).
9. Утвердить и ввести в действие Инструкцию о порядке резервирования и восстановления работоспособности технических средств,

программного обеспечения и средств защиты информации в информационных системах персональных данных МАУ «НЦВСМ» (Приложение 9).

10. Утвердить и ввести в действие Инструкцию об организации учета, хранения и выдачи машинных носителей персональных данных в информационных системах персональных данных МАУ «НЦВСМ» (Приложение 10).

11. Руководителям подразделений МАУ «НЦВСМ», участвующим в обработке персональных данных:

11.1. ознакомить под подпись с прилагаемыми документами работников, участвующих в обработке персональных данных;

11.2. организовать и вести работу по обеспечению обработки персональных данных в соответствии с нормами, изложенными в прилагаемых документах.

12. Контроль исполнения данного приказа возложить на ответственного за организацию обработки персональных данных в МАУ «НЦВСМ» - заместителя генерального директора по неолимпийским видам спорта Кабанова Павла Германовича.

Приложение:
1. Приложение 1 на 3 л. в 1 экз.;
2. Приложение 2 на 3 л. в 1 экз.
3. Приложение 3 на 2 л. в 1 экз.
4. Приложение 4 на 2 л. в 1 экз.
5. Приложение 5 на 3 л. в 1 экз.
6. Приложение 6 на 2 л. в 1 экз.
7. Приложение 7 на 1 л. в 1 экз.
8. Приложение 8 на 2 л. в 1 экз.
9. Приложение 9 на 4 л. в 1 экз.
10. Приложение 10 на 2 л. в 1 экз.

Генеральный директор В. Ф. Захаров

Зубахина
2252950

Лист согласования и ознакомления
к приказу № 01-02-17 от 18.03.2020
«Об утверждении инструкций и ознакомлении с ними ответственных лиц»

Согласовано:

№ п/п	Должность	Подпись	ФИО
1	заместитель генерального директора по кадровой и правовой работе		Дягилева О.Д.

С приказом ознакомлены:

№ п/п	Должность	Дата	Подпись	Фамилия, имя, отчество
1	заместитель генерального директора по олимпийским, паралимпийским, сурдолимпийским видам спорта	18.03.2020		Гусев А. А.
2	заместитель генерального директора по кадровой и правовой работе	23.03.20		Дягилева О. Д.
3	главный бухгалтер	18.03.20		Филоненко Л. В.
4	заместитель генерального директора структурного подразделения «Спортивный комплекс «Фламинго»	23 03 20		Митусов М. В.
5	заместитель генерального директора по неолимпийским видам спорта	18.03.2020		Кабанов П. Г.
6	заместитель генерального директора по административно-хозяйственной работе			Захарова В. С.
7	начальник финансового отдела	18.03.2020		Гусакова Т.Н.
8	начальник отдела кадров			Ломакина О. М.
9	начальник юридического отдела	18.03.2020		Зубахина О.В.
10	начальник отдела информационного обеспечения	18.03.20		Бобров М.И.

Приложение 1 к приказу от
«___»_____ 2020 г. №____

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция ответственного за организацию обработки персональных данных определяет основные обязанности, права и ответственность ответственного за организацию обработки персональных данных МАУ «НЦВСМ».

1.2. Ответственный за организацию обработки персональных данных (далее - уполномоченное лицо) назначается из числа сотрудников МАУ «НЦВСМ» приказом генерального директора МАУ «НЦВСМ» и осуществляет методическое руководство сотрудников, имеющих доступ к ПДн в вопросах обеспечения безопасности персональных данных.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных (далее – ПДн) и иной информации ограниченного распространения (далее – защищаемая информация), и не исключает обязательного выполнения их требований.

1.4. В своей деятельности уполномоченное лицо руководствуется Федеральным законом от 27.07.2006 г. № 152-ФЗ и иными нормативными правовыми актами в области защиты ПДн, приказами руководителя МАУ «НЦВСМ», а также настоящей должностной инструкцией.

1.5. Уполномоченное лицо несет персональную ответственность за качество проводимых им работ по контролю действий сотрудников, имеющих санкционированный доступ к ПДн.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.3. **Доступ к информации** – возможность получения информации и её использования.

2.4. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. **Информация** - сведения (сообщения, данные) независимо от формы их представления.

2.6. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.8. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

2.9. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.10. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.11. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.12. **Угрозы безопасности персональных данных (УБПДн)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

2.13. **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

III. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Уполномоченное лицо обязано:

3.1. Знать перечень и условия обработки персональных данных в МАУ «НЦВСМ».

3.2. Знать и предоставлять на утверждение генерального директора МАУ «НЦВСМ» изменения списка лиц, доступ которых к персональным данным необходим для выполнения ими своих трудовых обязанностей.

3.3. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

3.4. Осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения.

3.5. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.6. Реагировать на попытки несанкционированного доступа к информации в установленном ст.4 настоящей Инструкции порядке.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

3.8. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и правилам обработки персональных данных.

3.9. Проводить занятия и инструктажи с работниками МАУ «НЦВСМ» о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных.

3.10. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.11. Контролировать соблюдение сотрудниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными.

3.12. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.13. Организовать учет обращений субъектов персональных данных, контролировать заполнение «Журнала учета обращений субъектов персональных данных».

3.14. Представлять интересы МАУ «НЦВСМ» при проверках надзорных органов в сфере обработки персональных данных.

3.15. Знать законодательство РФ о персональных данных, следить за его изменениями.

3.16. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. К попыткам несанкционированного доступа относятся:

- сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных обязан:

- прекратить несанкционированный доступ к персональным данным;

- доложить генеральному директору МАУ «НЦВСМ» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

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

- известить администратора безопасности ИСПДн о факте несанкционированного доступа.

V. ПРАВА

Уполномоченное лицо имеет право:

5.1. Требовать от сотрудников выполнения локальных нормативно-правовых актов в части работы с персональными данными.

5.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

5.3. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VI. ОТВЕТСТВЕННОСТЬ

6.1. Уполномоченное лицо несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

6.2. Уполномоченное лицо при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 2 к приказу от
«___»_____ 2020 г. №____

Инструкция
администратора безопасности информационных систем муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

Общие положения

Настоящая Инструкция администратору безопасности информационных систем МАУ «НЦВСМ» (далее – Инструкция) определяет функции, права и обязанности администратора безопасности информационных систем МАУ «НЦВСМ» (далее – ИС).

Администратор безопасности ИС назначается из числа сотрудников МАУ «НЦВСМ» приказом генерального директора МАУ «НЦВСМ» и обеспечивает правильность использования и нормальное функционирование системы защиты информации информационных систем (далее – СЗИ ИС).

Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных (далее – ПДн) и иной информации ограниченного распространения (далее – защищаемая информация), и не исключает обязательного выполнения их требований.

1. Основные функции администратора безопасности ИС

1.1. Контроль за выполнением требований действующих нормативных документов по защите информации, обрабатываемой в ИС.

1.2. Контроль за порядком доступа лиц в помещение, где установлены компоненты ИС, в соответствии с Перечнем лиц, имеющих право доступа в помещения, в которых расположены технические средства информационных систем МАУ «НЦВСМ».

1.3. Настройка и сопровождение в процессе эксплуатации подсистемы идентификации и аутентификации субъектов доступа и объектов доступа.

1.3.1. Управление идентификаторами (именами учётных записей пользователей), в том числе создание, присвоение, уничтожение идентификаторов. При этом администратор информационной безопасности:

- формирует уникальный идентификатор (логин), который однозначно идентифицирует пользователя;
- присваивает идентификатор пользователю ИС на основании Перечня лиц, допущенных к работе в ИС;
- следит за исключением повторного использования идентификатора пользователя в период выполнения пользователем должностных обязанностей;
- заблаговременно блокирует идентификатор пользователя на период долговременного отсутствия пользователя;
- блокирует идентификатор пользователя через период времени неиспользования – 45 дней;
- исключает повторное использование идентификатора пользователя в течение трёх лет.

1.3.2. Управление средствами аутентификации (паролями), в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. Порядок управление средствами аутентификации определён в Инструкции по организации парольной защиты в информационных системах МАУ «НЦВСМ».

1.4. Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом субъектов доступа к объектам доступа.

1.4.1. Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей. При этом администратор информационной безопасности:

- определяет тип учётной записи (внутреннего пользователя, системная, приложения);
- осуществляет объединение учётных записей в группы (при необходимости);

- осуществляет верификацию пользователя (проверку личности пользователя, его должностных (функциональных) обязанностей) при заведении учётной записи пользователя;
- присваивает учётную запись конкретному пользователю ИС;
- предоставляет пользователю права доступа к объектам доступа ИС в соответствии с Разрешительной системой доступа субъектов доступа к объектам доступа ИС;
- при необходимости производит корректировку учётных записей пользователей;
- удаляет учётную запись пользователя при его увольнении;
- на период длительного отсутствия пользователя блокирует его учётную запись в средствах защиты информации от несанкционированного доступа.

1.4.2. Разработка и поддержание в актуальном состоянии Разрешительной системы доступа субъектов к объектам доступа ИС.

1.4.3. Реализация необходимых методов (дискреционный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа на основании Разрешительной системы доступа субъектов к объектам доступа ИС.

1.4.4. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС на основании Разрешительной системы доступа субъектов к объектам доступа ИС.

1.4.5. Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС на основании Разрешительной системы доступа субъектов к объектам доступа ИС.

1.4.6. Ограничение неуспешных попыток входа в ИС (3 неуспешные попытки входа).

1.4.7. Запрет действий пользователей в ИС до идентификации и аутентификации.

1.4.8. Контроль использования в ИС мобильных технических средств.

1.4.9. Контроль осуществления взаимодействия с информационными системами сторонних организаций (внешние информационные системы).

1.5. Настройка и сопровождение подсистемы регистрации событий безопасности.

1.5.1. Определение событий безопасности, подлежащих регистрации, и сроков их хранения.

1.5.2. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

1.5.3. Установка в средствах защиты информации необходимых параметров регистрации событий безопасности.

1.6. Настройка и сопровождение подсистемы антивирусной защиты в соответствии с Инструкцией по организации антивирусной защиты в информационных систем МАУ «НЦВСМ».

1.7. Сопровождение подсистемы контроля (анализа) защищённости информации.

1.7.1. Контроль установки обновлений ПО, включая обновление ПО средств защиты информации.

1.8. Сопровождение подсистемы обеспечения целостности ИС и информации.

1.8.1. Настройка механизмов контроля целостности ПО, включая ПО средств защиты информации, реагирование на сбои при выполнении контроля целостности ПО, включая ПО средств защиты информации, а также на изменение контрольных сумм ПО, включая ПО средств защиты информации.

1.9. Настройка и сопровождение подсистемы защиты информационной системы, её средств, систем связи и передачи данных.

1.9.1. Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передачи (подготовке к передаче) по каналам связи, имеющим вывод за пределы контролируемой зоны, в том числе беспроводным каналам связи.

1.9.2. Контроль работы пользователей ИС в сетях общего пользования и (или) международного обмена (сети «Интернет») в соответствии с Инструкцией о порядке работы при подключении к информационно-телекоммуникационным сетям международного информационного обмена в ИС.

1.10. Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

1.11. Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены

1.12. Периодическое предоставление ответственному за защиту информации, в том числе за защиту информации, в том числе за обеспечение безопасности ПДн, отчёта о состоянии защищённости информации при её обработке в ИС, о нештатных ситуациях при работе в ИС, о допущенных пользователями ИС нарушениях установленных требований по обеспечению безопасности защищаемой информации.

2. Обязанности

Администратор безопасности ИС обязан:

- обеспечивать функционирование и поддерживать работоспособность СЗИ ИС в пределах возложенных на него функций;
- проводить инструктажи пользователей по правилам работы в ИС;
- в случае отказа средств защиты информации принимать меры по их восстановлению;
- докладывать ответственному за защиту информации, в том числе за обеспечение безопасности ПДн, о неправомерных действиях пользователей ИС, приводящих к нарушению требований по обеспечению безопасности защищаемой информации;
- проводить мероприятия по выявлению возможных каналов утечки защищаемой информации при эксплуатации ИС и подготовке предложений по совершенствованию СЗИ ИС;
- вести документацию на ИС в соответствии с требованиями нормативных документов.

3. Права

Администратор безопасности ИС имеет право:

- участвовать в служебных расследованиях по вопросам несоблюдения требований организационно-распорядительных документов по обеспечению безопасности защищаемой информации;
- требовать прекращения обработки защищаемой информации в ИС в случае нарушения установленного порядка работ или нарушения функционирования СЗИ ИС.

4. Ответственность

Администратор безопасности несет персональную ответственность за:

- неисполнение, несвоевременное или некачественное выполнение возложенных на него обязанностей по обеспечению безопасности защищаемой информации при её обработке в ИС;
- достоверность отчетных данных и других подготавливаемых материалов;
- качество работ по обеспечению безопасности защищаемой информации в соответствии с функциональными обязанностями;
- соблюдение режима конфиденциальности защищаемой информации при её обработке и хранении в ИС;
- соблюдение требований нормативных правовых актов, приказов, распоряжений и инструкций, определяющих порядок организации работ по обеспечению безопасности защищаемой информации.

Приложение 3 к приказу
от «___» _____ 2020 г. №_____

Инструкция

ответственному за защиту информации, в том числе за обеспечение безопасности персональных данных в информационных системах муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

1.1. Настоящая Инструкция ответственному за защиту информации, в том числе за обеспечение безопасности персональных данных в информационных системах МАУ «НЦВСМ», (далее – уполномоченное лицо, Инструкция) определяет обязанности, ответственность и права ответственного за защиту информации, в том числе за обеспечение безопасности персональных данных (далее – ПДн) в информационных системах МАУ «НЦВСМ» (далее – ИС).

1.2. Уполномоченное лицо назначается из числа работников МАУ «НЦВСМ» приказом генерального директора.

2. Обязанности Уполномоченного лица

2.1. Уполномоченное лицо обязано:

– осуществлять контроль за выполнением требований действующих нормативных документов по вопросам обеспечения безопасности ПДн и иной информации ограниченного распространения (далее – защищаемой информации) при их обработке в ИС;

– обеспечивать эксплуатацию ИС в соответствии с её назначением;

– вести и хранить документацию на ИС;

– вести учёт, хранение и выдачу машинных носителей информации;

– вести учёт средств защиты информации, используемых в ИС;

– организовать порядок доступа в ИС;

– осуществлять взаимодействие с администратором безопасности ИС в целях контроля состояния защищенности информации в ИС;

– контролировать качество и своевременность выполнения должностными лицами установленных требований по обеспечению безопасности защищаемой информации;

– контролировать соблюдение правил допуска сотрудников в помещения, в которых находятся компоненты ИС;

– контролировать проведение технического обслуживания ИС;

– контролировать внесение изменений в конфигурацию программных, технических средств ИС, а также средств защиты информации;

– принимать участие в организации и проведении расследований по фактам нарушений в области защиты информации и разработке предложений по устранению недостатков и предупреждению подобного рода нарушений.

3. Права уполномоченного лица

3.1. Уполномоченное лицо имеет право:

– требовать от сотрудников выполнение инструкций по обеспечению безопасности защищаемой информации при её обработке в ИС;

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности защищаемой информации, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических средств ИС;

– требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств защиты информации;

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

– участвовать в мероприятиях по осуществлению контроля защиты информации, в том числе обеспечения безопасности ПДн;

– участвовать в расследовании возникающих инцидентов безопасности защищаемой информации при её обработке в ИС.

По каждой предпосылке к утечке защищаемой информации для выяснения обстоятельств и причин невыполнения установленных требований должна проводиться расследование. Для проведения расследования назначается специальная комиссия. Комиссия обязана установить, имела ли место утечка защищаемой информации, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по обеспечению безопасности защищаемой информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования главный врач принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4. Ответственность уполномоченного лица

Уполномоченное лицо несёт персональную ответственность за:

– неисполнение, несвоевременное или некачественное выполнение возложенных на него обязанностей по обеспечению безопасности защищаемой информации при её обработке в ИС;

– достоверность отчетных данных и других подготавливаемых материалов;

– качество работ по обеспечению безопасности защищаемой информации в соответствии с функциональными обязанностями;

– соблюдение режима конфиденциальности защищаемой информации при её обработке и хранении в ИС;

– соблюдение требований нормативных правовых актов, приказов, распоряжений и инструкций, определяющих порядок организации работ по обеспечению безопасности защищаемой информации.

Приложение 4 к приказу от
«___» _____ 2020 г. №____

Инструкция
по работе пользователей в информационных системах муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. **Общие положения**

1.1. Настоящая Инструкция по работе пользователей в информационных систем МАУ «НЦВСМ» (далее – Инструкция) определяет задачи, функции, обязанности, права и ответственность пользователей, допущенных к работе в информационных системах МАУ «НЦВСМ» (далее – ИС).

1.2. Пользователями ИС являются сотрудники МАУ «НЦВСМ».

2. **Обязанности пользователя**

2.1. При эксплуатации ИС пользователь обязан:

2.1.1. Руководствоваться требованиями настоящей инструкции.

2.1.2. Помнить личные пароли.

2.1.3. Соблюдать установленную технологию обработки персональных данных и иной информации ограниченного распространения (далее – защищаемая информация).

2.1.4. Размещать устройства вывода информации средств вычислительной техники (далее – СВТ), информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИС, в помещении, в котором они установлены, таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей защищаемую информацию.

2.1.5. При возвращении на рабочее место контролировать целостность меток, исключающих негласное вскрытие системного блока СВТ и в случае нарушения целостности, сообщать об этом администратору безопасности ИС.

2.1.6. Препятствовать использованию СВТ лицами, не допущенными к работе в ИС.

2.2. При временном оставлении рабочего места пользователь обязан:

– блокировать ввод-вывод информации на своём рабочем месте ИС в случаях кратковременного отсутствия (перерыв) или выключать СВТ ИС;

– блокировать вывод информации на монитор СВТ;

2.3. При работе со съемными носителями информации, содержащими ПДн соблюдать режим конфиденциальности и следить за сохранностью носителей информации.

2.4. Пользователю ЗАПРЕЩАЕТСЯ:

– подключать к СВТ нештатные устройства;

– производить загрузку нештатной операционной системы с внешнего машинного носителя информации;

– самостоятельно вносить изменения в состав, конфигурацию и размещение СВТ ИС;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения (далее – ПО), установленного в ИС;

– устанавливать запрещённое к использованию ПО;

– самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации ИС, а так же завершать работу средств защиты информации ИС;

– сообщать устно, письменно или иным способом другим лицам пароли, передавать личные идентификаторы (наименование учётной записи), ключевые носители и другие реквизиты доступа к ресурсам ИС.

3. **Права**

Пользователь ИС имеет право:

– обращаться к администратору безопасности ИС с просьбой об оказании технической и методической помощи по обеспечению безопасности защищаемой

информации, обрабатываемой в ИС, по использованию установленных программных и технических средств ИС, а также по вопросам эксплуатации установленных средств защиты информации;

– обращаться к лицу, ответственному за защиту информации, в том числе за обеспечение безопасности персональных данных в ИС, по вопросам эксплуатации ИС (выполнение установленной технологии обработки защищаемой информации, инструкций и других документов по обеспечению безопасности защищаемой информации);

– обращаться к лицу, ответственному за защиту информации, в том числе за обеспечение безопасности персональных данных в ИС, по вопросам выполнения режимных мер при обработке защищаемой информации.

4. Ответственность

Пользователь несет персональную ответственность:

– за соблюдение установленной технологии обработки защищаемой информации;

– за соблюдение режима конфиденциальности при обработке защищаемой информации в ИС;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИС;

– за соблюдение требований нормативных правовых актов, приказов, распоряжений и указаний, определяющих порядок организации работ по обеспечению безопасности защищаемой информации.

Приложение 5 к приказу от
«___»_____ 2020 г. №____

Инструкция

о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации, в информационных систем муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

1.1. Настоящая Инструкция о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации, в информационных систем МАУ «НЦВСМ» (далее – Инструкция) определяет правила работ по техническому обслуживанию, ремонту, модернизации технических средств, а также обновления программного обеспечения в информационных системах МАУ «НЦВСМ» (далее – ИС).

1.2. Данные работы проводятся с разрешения генерального директора МАУ «НЦВСМ», после согласования с ответственным за защиту информации, в том числе за обеспечение безопасности персональных данных (далее – ПДн) в ИС.

2. Порядок проведения работ по техническому обслуживанию, ремонту, модернизации технических средств

2.1. В случае, когда необходимо провести работы по техническому обслуживанию (ремонту, модернизации) технических средств, входящих в состав ИС, ответственный за защиту информации, в том числе за обеспечение безопасности ПДн в ИС, представляет служебную записку, в которой:

- указывает название и номер автоматизированного рабочего места (далее – АРМ) (технического средства, системы), техническое обслуживание (ремонт, модернизацию) которого необходимо провести и с какой целью;
- обосновывает необходимость технического обслуживания (модернизации);
- указывает планируемые место и сроки работ, режим их проведения;
- перечисляет меры безопасности, которые будут реализованы при техническом обслуживании (ремонте, модернизации) с целью недопущения доступа к персональным данным посторонних лиц.

2.2. В случае если для проведения работ необходимо привлекать лиц, не имеющих постоянного допуска к работе в ИС, составляется список лиц, который согласовывается с генеральным директором МАУ «НЦВСМ».

2.3. Запрещается выносить технические средства, входящие в состав ИС, из помещения, в котором они расположены, без согласования с ответственным за защиту информации, в том числе за обеспечение безопасности ПДн в ИС, и разрешения генерального директора МАУ «НЦВСМ».

2.4. Вскрытие печатей на корпусе АРМ или других технических средств и последующее опечатывание производится комиссионно в присутствии ответственного за защиту информации, в том числе за обеспечение безопасности ПДн в ИС, о чём составляется акт.

В акте указывается:

- номер (название) помещения, в котором проводились работы;
- дата и время начала и окончания работ;
- лица, присутствовавшие при вскрытии и обслуживании (ремонте, модернизации);
- наличие, целостность и места размещения печатей (пломб, специальных защитных знаков) до вскрытия АРМ (технического средства, системы);
- установленные неисправности;
- виды и результаты проведенных работ;

- замененные или отремонтированные узлы (детали), наличие на этих узлах специальных защитных знаков;
- какими печатями (пломбами и т.д.) и в каких местах АРМ (устройство) опечатано по окончании работ;
- иная необходимая для дальнейшей работы и обеспечения безопасности информация.

2.5. Если для ремонта (модернизации) АРМ (другого технического средства, системы, элемента АРМ в составе ИС) необходимо направить в специализированную организацию, то комиссией составляется заключение.

2.6. Перед отправкой АРМ (другого технического средства, системы, элемента АРМ) ответственный за защиту информации, в том числе за обеспечение безопасности ПДн в ИС, обязан изъять накопитель на жёстком диске и иные устройства памяти из состава АРМ, в случае необходимости передачи накопителя на жёстком диске и (или) иных устройств памяти, хранящиеся на них персональные данные и иную информацию ограниченного распространения (далее – защищаемая информация), необходимо гарантированно удалить сертифицированными средствами или произвести их обезличивание.

2.7. Изъятые устройства опечатываются и хранятся у ответственного за защиту информации, в том числе за обеспечение безопасности ПДн в ИС, с соблюдением требований, предъявляемых к хранению защищаемой информации.

2.8. Ремонт и замена накопителя на жёстком диске производится с соблюдением требований п. п. 2.5.-2.7. настоящей Инструкции в присутствии ответственного за защиту информации, в том числе за обеспечение безопасности ПДн в ИС. При диагностике и ремонте накопителя на жёстком диске должны быть реализованы меры безопасности, исключающие несанкционированный доступ к хранящимся на нём данным.

3. Порядок обновления общесистемного и прикладного программного обеспечения

3.1. Установку, обновление и модификацию общесистемного и прикладного программного обеспечения ИС проводит администратор безопасности ИС.

3.2. Изменение конфигурации программных средств ИС кем-либо, кроме администратора безопасности ИС, запрещено.

3.3. Установка или обновление программного обеспечения ИС должны проводиться в строгом соответствии с технологией проведения модификаций программного обеспечения.

3.4. Установка и обновление программного обеспечения (системного, прикладного, тестового и т.п.) в ИС производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), если иной порядок установки обновления не предусмотрен разработчиком программного обеспечения.

3.5. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.

3.6. Программное обеспечение, устанавливаемое на АРМ и сервера ИС, а также его обновления, перед установкой должны пройти антивирусную проверку.

4. Порядок обновления программного обеспечения средств защиты информации

4.1. Обновление баз данных, необходимых для реализации функций безопасности средства защиты информации (обновление баз сигнатур вирусов средств антивирусной защиты, баз решающих правил систем обнаружения вторжений и других средств защиты информации) выполняется в автоматическом режиме по расписанию со специальных серверов обновления производителей средств защиты информации.

4.2. Обновление, направленное на добавление функции (функций) безопасности средства защиты информации, на совершенствование реализации функции (функций)

безопасности средства защиты информации, на расширение числа поддерживаемых программных и аппаратных платформ, а также обновление, не влияющее на безопасность средства защиты информации (изменение интерфейса средства защиты информации, иных функций, не влияющее на функции безопасности средства защиты информации) осуществляются по решению генерального директора МАУ «НЦВСМ» в порядке, определённом производителем средства защиты информации.

4.3. Внесение изменений в конфигурацию аппаратно-программных средств защиты информации осуществляет администратор безопасности ИС после согласования с ответственным за защиту информации, в том числе за обеспечение безопасности ПДн в ИС.

Приложение 6 к приказу от
«___» _____ 2020 г. №___

Инструкция
по организации антивирусной защиты в информационных системах муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие требования

1.1. Настоящая Инструкция по организации антивирусной защиты в информационных системах МАУ «НЦВСМ» (далее – Инструкция) определяет требования к организации защиты информационных систем МАУ «НЦВСМ» (далее – ИС) от разрушающего воздействия вредоносных компьютерных программ (компьютерных вирусов) и устанавливает ответственность МАУ «НЦВСМ», эксплуатирующих и сопровождающих ИС, за их выполнение.

1.2. К использованию в ИС допускаются только средства антивирусной защиты прошедшие в установленном порядке процедуру оценки соответствия.

1.3. Установка и настройка средств антивирусной защиты осуществляется специально назначенным лицом (администратором безопасности ИС), в соответствии с руководствами по применению конкретных средств антивирусной защиты.

2. Применение средств антивирусной защиты

2.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на оптических компакт-дисках перед копированием в ИС.

2.2. Накопители на жёстких дисках и оперативная память автоматизированных рабочих мест (далее – АРМ) и серверов должны находится под постоянным контролем средства антивирусной защиты.

2.3. Полная проверка всех файлов ИС должна выполняться не реже одного раза в неделю, а также по запросу пользователя ИС.

2.4. Быстрая проверка файлов ИС должна выполняться автоматически после запуска средства антивирусной защиты.

2.5. Должна проводиться автоматическая проверка подключаемых машинных носителей информации.

2.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения, администратором безопасности ИС должна быть выполнена антивирусная проверка АРМ и (или) серверов.

2.7. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИС самостоятельно или вместе с администратором безопасности ИС должен провести внеочередную антивирусную проверку своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности ИС;
- провести анализ необходимости дальнейшего использования зараженных файлов;
- провести лечение или уничтожение зараженных файлов.

2.8. Обновление базы данных средства антивирусной защиты должно осуществляться регулярно в автоматическом режиме со специального сервера обновлений средства антивирусной защиты.

3. Ответственность

3.1. Ответственность за организацию и проведение мероприятий по антивирусной защите в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

3.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на пользователя ИС.

3.3. Периодический контроль за состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусной защиты и выполнением требований настоящей Инструкции осуществляется администратором безопасности ИС.

Приложение 7 к приказу от
«___» _____ 2020 г. №__

Инструкция
по организации криптографической защиты в информационных системах муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие требования

1.1. Настоящая Инструкция по организации криптографической защиты в информационных системах МАУ «НЦВСМ» (далее – Инструкция) определяет требования к организации защиты информационных систем МАУ «НЦВСМ» (далее – ИС) обеспечивает информационную безопасность и позволяет гарантировать высокий уровень сохранности данных, для хранения корпоративных данных и обмена ими, устанавливает ответственность МАУ «НЦВСМ», эксплуатирующих и сопровождающих ИС.

1.2. К использованию в ИС допускаются только средства криптографической защиты прошедшие в установленном порядке процедуру оценки соответствия.

1.3. Установка и настройка средств криптографической защиты осуществляется специально назначенным лицом (администратором безопасности ИС), в соответствии с руководствами по применению конкретных средств криптографической защиты.

2. Обязанности администратора безопасности ИС

2.1. Ответственный за эксплуатацию СКЗИ обязан:

- обеспечивать конфиденциальность всей информации ограниченного распространения, в том числе сведения о криптографических ключах;
- не допускать снятия копий с ключевых документов;
- не допускать записи посторонней информации на ключевой носитель;
- получать от пользователей носители ключевой информации при их увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- получать от пользователей носители ключевой информации по окончании срока действия сертификата ключа, а также в случае компрометации ключа;
- проводить расследования по факту недостачи или утраты СКЗИ, криптографических ключей, ключей от помещений, хранилищ, личных печатей и в других случаях, которые могут привести к разглашению защищаемой информации;
- останавливать работу пользователей на ПЭВМ в случаях обнаружения неисправностей.

2.2. Ответственному за эксплуатацию СКЗИ запрещается:

-осуществлять копирование криптографических ключей;
- допускать использование ключевых носителей на других рабочих местах или для использования в целях, не относящихся к работе;
- допускать хранение ключевых носителей вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;
- допускать передачу ключевых носителей каким бы то ни было лицам;
- допускать использование в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации;
- допускать разглашение содержимого ключевых носителей и вывод ключевой информации на дисплей или принтер;
- допускать вставку носителей криптографических ключей в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ;
- записывать на носители с криптографическими ключами постороннюю информацию;
- допускать подключение к ПЭВМ дополнительных устройств и соединителей, непредусмотренных в комплектации;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- допускать работу на ПЭВМ при отключенных средствах антивирусной защиты.

4. Права администратора безопасности ИС

4.1. Ответственный за эксплуатацию СКЗИ имеет право:

- вносить предложения руководству по совершенствованию СКЗИ;
- повышать уровень квалификации по использованию СКЗИ.

5. Ответственность

5.1. Ответственность за организацию и проведение мероприятий по криптографической защите в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

5.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на пользователя ИС.

5.3. Периодический контроль за состоянием криптографической защиты в ИС, а также за соблюдением установленного порядка криптографической защиты и выполнением требований настоящей Инструкции осуществляется администратором безопасности ИС.

Приложение 8 к приказу от
«___»_____ 2020 г. №____

Инструкция
по организации парольной защиты в информационных системах муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

1.1. Настоящая Инструкция по организации парольной защиты в информационных системах МАУ «НЦВСМ» (далее – Инструкция) определяет порядок использования, генерации, смены и прекращения действия паролей пользователей в информационных системах МАУ «НЦВСМ» (далее – ИС), а также контроль действий пользователя при работе с паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль за реализацией требований по обеспечению безопасности при использовании паролей возлагается на администратора безопасности ИС.

2. Требования к организации парольной защиты

2.1. Установку первичного пароля производит администратор безопасности ИС при создании новой учётной записи. Ответственность за сохранность первичного пароля лежит на администраторе безопасности информации.

2.2. При создании первичного пароля, администратор безопасности ИС обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учётной записи о необходимости произвести смену пароля.

2.3. Первичный пароль так же используется при сбросе забытого пароля на учётную запись.

2.4. Установку основного пароля производит пользователь при первом входе в систему с новой учётной записью.

2.5. Устанавливаемые пароли должны соответствовать следующим требованиям:

– длина пароля должна быть не менее 8 символов;

– пароль должен содержать строчные и прописные буквы, а также небуквенные символы (цифры, знаки пунктуации, специальные символы).

– использование трех и более, подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;

– использование в качестве пароля одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов недопустимо;

– новое значение пароля не должно совпадать с одним из трех предыдущих значений;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования автоматизированного рабочего места, имя учётной записи или какую-либо его часть, общепринятые сокращения (password, USER, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

2.6. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом администратору безопасности ИС и изменить пароль.

2.7. Восстановление забытого пароля пользователя осуществляется администратором безопасности ИС на основании письменной либо электронной заявки пользователя.

2.8. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

2.9. Для предотвращения несанкционированного доступа в ИС должен быть реализован механизм блокировки учётной записи при трёхкратном неправильном вводе пароля на 10 минут.

2.10. Должен быть установлен пароль на доступ к настройкам используемых средств защиты информации. Указанный пароль должен отвечать требованиями к сложности паролей (п.2.5 Инструкции).

2.11. Пользователи и администратор безопасности ИС обязаны:

– сохранять в тайне свои личные пароли;

– четко знать и строго выполнять требования настоящей Инструкции;

– своевременно сообщать лицу, ответственному за защиту информации, в том числе за обеспечение безопасности персональных данных в ИС, обо всех нештатных ситуациях, нарушениях работы подсистем защиты от несанкционированного доступа, возникающих при работе с паролями.

2.12. При организации парольной защиты запрещается:

– записывать свои пароли на любой носитель;

– хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги на рабочем месте;

– сообщать посторонним лицам свои пароли, а также пересылать открытым текстом в электронных сообщениях.

3. Порядок применения парольной защиты

3.1. Полная плановая смена паролей производится регулярно, не реже одного раза в 90 дней. При плановой смене пароля, пользователь самостоятельно меняет свой пароль.

3.2. Внеплановая смена (удаление) личного пароля любого пользователя производится в следующих случаях:

– по окончании срока действия пароля;

– в случае прекращения полномочий пользователя (увольнение, переход на другую работу внутри МАУ «НЦВСМ»);

– при обнаружении факта успешной попытки несанкционированного доступа к элементам ИС;

– при обнаружении факта компрометации пароля.

3.3. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности ИС.

3.4. Скомпрометированные пароли выводятся из действия немедленно.

3.5. По каждому случаю, связанному с компрометацией действующих паролей, ответственным за защиту информации, в том числе за обеспечение безопасности персональных данных в ИС, организуется и проводится служебное расследование.

3.6. Результаты служебного расследования в виде служебной записки предоставляются генеральному директору МАУ «НЦВСМ». По результатам расследования лица, допустившие разглашение паролей, привлекаются к дисциплинарной ответственности.

Приложение 9 к приказу от
«___» _____ 2020 г. №____

Инструкция

о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и средств защиты информации в информационных системах муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Общие положения

1.1. Настоящая Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения и средств защиты информации в информационных системах персональных данных МАУ «НЦВСМ» (далее – Инструкция) определяет порядок действий по резервированию и восстановлению работоспособности технических средств (далее – ТС) и программного обеспечения (далее – ПО), средств защиты информации (далее – СЗИ), связанных с функционированием информационной системы персональных данных (далее – ИСПДн) МАУ «НЦВСМ», меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью Инструкции является превентивная защита элементов ИСПДн от потери защищаемой информации.

1.3. Задачами данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей МАУ «НЦВСМ», имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.5. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности ИСПДн.

1.6. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается администратор безопасности ИСПДн или ответственный за защиту информации, в том числе за обеспечение безопасности персональных данных.

2. Порядок реагирования на инцидент

2.1. В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником.

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности информации, предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры:

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.1.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации;
- системы резервного питания.

3.1.3. Все критичные помещения МАУ «НЦВСМ» (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации.

3.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- резервные линии электропитания в пределах комплекса зданий.

3.1.5. Система резервного копирования ИС «Зарплата и кадры» и «Бухгалтерия государственного учреждения», подразумевает под собой создание копий защищаемой информации. Создание резервных копий осуществляется при помощи стандартных средств Операционной системы или других программных средств на съемный носитель информации, который должен быть учтен в «Журнале учета носителей персональных данных».

3.2. Организационные меры:

3.2.1. Резервное копирование данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в 6 месяцев, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Данные о проведение процедуры резервного копирования и восстановления, должны отражаться в специально созданном журнале учета.

3.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2.4. Носители должны храниться в несгораемом шкафу (сейфе).

3.2.5. Носители должны храниться не менее года, для возможности восстановления данных.

4. Порядок восстановления работоспособности информационных систем

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы, в общем случае, осуществляются в следующей последовательности:

- проверка исправности и работоспособности средств обеспечения функционирования ИСПДн;
- восстановление работоспособности (ремонт или замена) средств обеспечения функционирования ИСПДн, при необходимости;
- проверка правильности функционирования общего программного обеспечения ИСПДн;
- восстановление нормального функционирования общего программного обеспечения ИСПДн с использованием дистрибутивов и обновлений к ним или резервных копий настроек, при необходимости;
- проверка правильности функционирования средств защиты информации;
- восстановление нормального функционирования средств защиты информации с использованием дистрибутивов и обновлений к ним, при необходимости;
- проверка правильности функционирования специального программного обеспечения ИСПДн;
- восстановление нормального функционирования специального программного обеспечения ИС с использованием дистрибутивов и обновлений к ним, при необходимости;
- восстановление баз персональных данных с использованием резервной копии в течении одного рабочего дня.

Данные работы осуществляются в соответствии с эксплуатационной документацией на технические и программные средства до полного восстановления работоспособности.

Восстановление персональных данных, созданных после их последнего резервирования, осуществляется пользователями, осуществившими их внесение в базы персональных данных.

Работы по техническому обслуживанию технических и программных средств ИСПДн осуществляется в соответствиями с правилами, установленными в «Инструкции о порядке технического обслуживания, ремонта, модернизации технических средств, а также обновления программного обеспечения, включая обновление программного обеспечения средств защиты информации ИСПДн».

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными, а также несанкционированного копирования на машинные носители информации. Ответственность за выполнение данного требования возлагается на администратора безопасности информации.

Приложение к Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах МАУ «НЦВСМ»

Форма
журнала резервирования и восстановления работоспособности технических средств и программного обеспечения, и средств защиты информации

№	Дата	Вид операции	Устройство	Каталог накопителя	Наименование резервной копии	Место хранения резервной копии	ФИО, проводившего резервирование / восстановление	Подпись, проводившего резервирование / восстановление

Приложение 10 к приказу от
«___» _____ 2020 г. №____

Инструкция

об организации учёта, хранения и выдачи машинных носителей персональных данных в информационных системах муниципального автономного учреждения города Новосибирска «Новосибирский Центр Высшего Спортивного Мастерства»

1. Настоящая Инструкция об организации учёта, хранения и выдачи машинных носителей персональных данных информационных системах персональных данных МАУ «НЦВСМ» (далее – Инструкция) устанавливает организацию учета, хранения и выдачи машинных персональных данных информационных систем персональных данных МАУ «НЦВСМ» (далее – ИСПДн).

2. Учёт, хранение и выдачу машинных носителей персональных данных (далее – МНПДн) осуществляет ответственный за обеспечение безопасности персональных данных в ИСПДн. При увольнении сотрудника, ответственного за учёт, хранение и выдачу машинных носителей персональных данных, составляется акт приема-сдачи журналов учёта, который утверждается руководителем МАУ «НЦВСМ».

3. Виды и типы машинных носителей персональных данных МНПДн в ИСПДн являются МНПДн, встроенные в корпус средств вычислительной техники (накопители на жёстких дисках), съёмные МНПДн (флэш-накопители) и оптические компакт-диски.

4. Организация учёта машинных носителей персональных данных.

Учёту подлежат МНПДн, встроенные в корпус средств вычислительной техники (накопители на жёстких дисках) и съёмные МНПДн (флэш-накопители).

Учёт МНПДн производится в Журнале учёта машинных носителей персональных данных (форма журнала приведена в Приложении к Инструкции).

Учёт МНПДн включает присвоение регистрационных (учётных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих МНПДн, номера инвентарного учёта, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

5. Организация выдачи машинных носителей персональных данных:

Пользователи ИСПДн получают съёмные МНПДн у ответственного за обеспечение безопасности персональных данных в ИСПДн.

6. Организация хранения машинных носителей персональных данных

Хранение МНПДн осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение содержащихся на нем персональных данных, а также хищение носителей. Носители должны храниться в служебных помещениях в сейфах или металлических хранилищах. Запрещается хранить МНПДн на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

7. В случае утраты МНПДн, либо разглашения содержащихся в них сведений, немедленно ставится в известность ответственный за обеспечение безопасности персональных данных в ИСПДн.

8. МНПДн, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. По результатам уничтожения МНПДн составляется Акт уничтожения машинных носителей персональных данных.

9. При передаче средств вычислительной техники ИСПДн сторонним организациям для проведения ремонтно-восстановительных или иных работ встроенный МНПДн изымается из состава средств вычислительной техники, в случае необходимости передачи МНПДн, хранящиеся на нем персональные данные, необходимо гарантированно удалить сертифицированными средствами или произвести их обезличивание.

10. Ответственность за выполнение правил эксплуатации МНПДн при выполнении непосредственных работ с МНПДн несёт пользователь ИСПДн.

11. Контроль выполнения пользователями установленных правил эксплуатации МНПДн, осуществляет ответственный за обеспечение безопасности персональных данных в ИСПДн и администратор безопасности ИСПДн в рамках своих должностных обязанностей.

Приложение к Инструкции об организации учета, хранения и выдачи машинных носителей персональных данных информационных систем персональных данных МАУ «НЦВСМ»

Форма журнала учёта машинных носителей персональных данных

Журнал начат «____» _____ 20___ г. Журнал завершен «____» _____ 20___ г.

_____ / ФИО, должность / _____ / ФИО, должность /

На _____ листах

№ п/п	Регистрационный номер/дата	Тип/ёмкость машинного носителя персональных данных/серийный номер	Номер экземпляра/ количество экземпляров	Место установки (использования)/дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)
1									
2									
…									
N									