Приложение № 1к Приказу от 10.04.2014 №169

ИНСТРУКЦИЯ
по резервному копированию и восстановлению персональных данных

1. Общие положения

1.1. Настоящая Инструкция разработана с целью уменьшения ущерба от несанкционированного изменения (удаления) информации во время обработки и хранения персональных данных (ПДн) обрабатываемых в информационных системах персональных данных (ИСПДн) Управления образования Администрации Турочакского района МО «Турочакский район» и определяет порядок:

− резервного копирования (резервирования) информации содержащей ПДн для последующего восстановления;

− восстановления информации в случае возникновения такой необходимости.

1.2. Организация резервирования информации должна обеспечивать сохранность ПДн и возможность восстановления работы с информацией в максимально сжатые сроки.

2. Порядок резервного копирования

2.1. Организация резервного копирования информации производится исходя из следующих параметров:

− состав и объем копируемых данных;

− периодичность проведения резервного копирования;

− максимальный срок хранения резервных копий.

2.2. Порядок резервного копирования информации должен обеспечивать сохранность информации, достаточную для поддержания в актуальном состоянии обрабатываемых и хранящихся ПДн.

2.3. Ответственными за резервное копирование информации, содержащей ПДн, в Управлении образования Администрации Турочакского района МО «Турочакский район» является системный администратор, ответственный за информационную безопасность.

2.4. Состав резервируемой информации определяется специалистами, обрабатывающими данную информацию, периодичность резервирования и срок хранения резервных копий информации содержащей ПДн определяется системным администратором, ответственным за информационную безопасность.

2.5. Резервное копирование информации содержащей ПДн производится путем копирования информации на резервный носитель:

- «1С Бухгалтерия» - по мере обновления информации;
- «1С Кадры» - по мере обновления информации;
- «Сбис» - по мере обновления информации;
- «Электронная очередь» - по мере обновления информации.

2.6. Контроль результатов резервного копирования осуществляется исполнителем по окончании процедуры резервного копирования.

2.7. В случае обнаружения ошибок лицо, проводившее резервное копирование, повторно проводит данную процедуру.

2. Восстановление информации из резервных копий

3.1. Восстановление информации из резервных копий производится программистом, ответственным за информационную безопасность.

3.2. О фактах, связанных с необходимостью восстановления информации, ставится в известность специалист по защите информации (администратор ИСПДн), который в свою очередь анализирует сложившуюся ситуацию и принимает соответствующие меры по недопущению подобных инцидентов в будущем.
3.3. В случае отсутствия возможности самостоятельно восстановить информацию программист сообщает об этом администратору ИСПДн, который принимает меры по восстановлению информации в соответствии со сложившейся ситуацией.

3. Заключительные положения

4.1. В качестве новых носителей информации допускается повторно использовать те, у которых срок хранения содержащейся информации истек.
4.2. Информация с носителей, которые перестают использоваться в системе резервного копирования, должна стираться.

Приложение №2к Приказу от 10.04.2014 №169

Порядок
обеспечения безопасности персональных данных с использованием криптосредств при их обработке в информационных системах

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
2. Обеспечение безопасности персональных данных достигается, в частности:
1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных (Крипто PRO, TOKKEN);
3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
5) учетом машинных носителей персональных данных;
6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.
3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:
1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.
4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 статьи 19 ФЗ «О персональных данных» требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются

федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

7. Проекты нормативных правовых актов, указанных в части 5 статьи 19 ФЗ «О персональных данных», подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами

персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Исходный класс защищенности – средний.

Таблица 1

Наименование угрозы	Вероятность реализации угрозы (Y_2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1. Угрозы утечки акустической информации	маловероятная	Средняя	Низкая	Неактуальная	Виброгенераторы, генераторы шумов, звукоизоляция.	Инструкция пользователя Технологический процесс
1.2. Угрозы утечки видовой информации	маловероятная	Низкая	Низкая	Неактуальная	Жалюзи на окна	Пропускной режим Инструкция пользователя
2. Угрозы несанкционированного доступа к информации						
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн						
2.1.1. Кража ПЭВМ	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация Шифрование данных	Пропускной режим Охрана Акт установки средств защиты
2.1.2. Кража носителей информации	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация Хранение в сейфе	Акт установки средств защиты Учет носителей информации

					Шифрование данных	
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Низкая	Неактуальная	Хранение в сейфе	Инструкция пользователя
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Акт установки средств защиты
					Шифрование данных	
					Система защиты от НСД	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Низкая	Неактуальная	Охранная сигнализация	Пропускной режим
2.1.6. Несанкционированное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция администратора безопасности
						Технологический процесс обработки
						Акт установки средств защиты
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);						
2.2.1. Действия вредоносных программ (вирусов)	Низкая	Средняя	Высокая	Актуальная	Антивирусное ПО	Инструкция пользователя
						Инструкция ответственного
						Инструкция администратора безопасности

						Технологический процесс обработки Инструкция по антивирусной защите Акт установки средств защиты
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Высокая	Средняя	Средняя	Актуальная		Сертификация
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	Инструкция пользователя Инструкция ответственного
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.						
2.3.1. Утрата ключей и атрибутов доступа	Низкая	Средняя	Средняя	Актуальная		Инструкция пользователя Инструкция администратора безопасности
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Маловероятно	Низкая	Низкая	Неактуальная	Настройка средств защиты	**Резервное копирование**
2.3.3. Непреднамеренное отключение средств защиты	Маловероятно	Низкая	Низкая	Неактуальная	Доступ к установлению режимов работы средств защиты предоставляется только администратору безопасности	Инструкция пользователя Инструкция администратора безопасности
2.3.4. Выход из строя аппаратно-программных средств	Маловероятно	Низкая	Низкая	Неактуальная		Резервирование

2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная		Резервное копирование
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная	Пожарная сигнализация	
2.4. Угрозы преднамеренных действий внутренних нарушителей						
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	Маловероятно	Низкая	Низкая	Неактуальная	Система защиты от НСД	Акт установки средств защиты Разрешительная система допуска Технологический процесс обработки
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая	Средняя	Низкая	Неактуальная		Договор о не разглашении Инструкция пользователя
2.5. Угрозы несанкционированного доступа по каналам связи						

Таким образом, актуальными угрозами безопасности ПДн в Управлении образования Администрации Турочакского района МО «Турочакский район», являются:

- угрозы наличия недекларированных возможностей системного ПО и ПО для обработки персональных данных;
- угрозы перехвата за переделами с контролируемой зоны
- угрозы сканирования;
- угрозы утраты ключей и атрибутов доступа;
- угрозы выявления паролей по сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ;

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

- парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;
- назначить ответственного за безопасность персональных данных из числа сотрудников учреждения;
- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;
- убрать подключение элементов ИСПДн к сетям общего пользования и (или) международного обмена (сеть Интернет), если это не требуется для функционирования ИСПДн;
- осуществление резервирования ключевых элементов ИСПДн;
- организация физической защиты каналов передачи данных;
- если производится передача обрабатываемой информации по каналам связи, то необходимо использовать шифрование;
- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.