Бакаева Жамал Николаевна

Подписано Цифровой подписью: Бакаева Жамал Николаевна

ИНСТРУКЦИЯ
о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций

1. Общие положения

Настоящая Инструкция предназначена для определения порядка действий пользователей информационных системы персональных данных (ИС) данных Государственном бюджетном дошкольном образовательном учреждении детский сад № 15 Центрального района Санкт-Петербурга (далее – ГБДОУ) при возникновении нештатных ситуаций.

1.1. Нештатными ситуациями являются:

1) разглашение информации ограниченного доступа, не составляющей государственную тайну (далее–защищаемая информация), сотрудниками ГБДОУ, имеющими к ней право доступа, в том числе:

- разглашение информации лицам, не имеющим права доступа к защищаемой информации;
- передача защищаемой информации по открытым линиям связи;
- обработка защищаемой информации на незащищенных технических средствах (ТС) обработки информации;
- опубликование защищаемой информации в открытой печати и других средствах массовой информации;
- передача носителя информации лицу, не имеющему права доступа к ней;
- утрата носителя с защищаемой информацией;

2) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- несанкционированное изменение защищаемой информации;
- несанкционированное копирование защищаемой информации.

3) несанкционированный доступ к защищаемой информации:

- подключение ТС к средствами системам объекта информатизации;
- использование закладочных устройств;
- маскировка под зарегистрированного пользователя;
- использование дефектов программного обеспечения (ПО) объекта информатизации (ОИ);
- использование программных закладок;
- применение программных вирусов;
- хищение носителя защищаемой информации;

– нарушение функционирования ТС обработки информации;

– блокирование доступа к защищаемой информации путем перегрузки ТС обработки информации ложными заявками на ее обработку;

4) дефекты, сбои, отказы, аварии ТС и систем ОИ;

5) дефекты, сбои и отказы ПООИ;

6) сбои, отказы и аварии систем обеспечения ОИ;

7) природные явления, стихийные бедствия:

– термические, климатические факторы (пожары, наводнения и т.д.);

– механические факторы (землетрясения и т.д.);

– электромагнитные факторы (грозовые разряды и т.д.).

1.2. В случае возникновения нештатной ситуации, порядок действий, при которой не регламентирован настоящей инструкцией администратором информационной безопасности (АИБ) ИС, ответственный за обработку персональных данных ГБДОУ, вырабатывается конкретный план действий с учетом текущей ситуации.

1.3. Резервируемые в ГБДОУ информационные ресурсы и способы их резервирования представлены в Приложении 1 к настоящей Инструкции.

1.4. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении 2 к настоящей Инструкции.

1.5. Для эффективной реализации мероприятий по реагированию в случае нештатных ситуаций должны проводиться регулярные инструктажи по действиям в различных нештатных ситуациях.

1.6. Должностные лица ГБДОУ знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

1.7. Ознакомление с требованиями Инструкции сотрудников ГБДОУ осуществляет ответственный за обработку персональных данных под подпись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

2. Порядок действий при обнаружении нештатных ситуаций

2.1. Классификация нештатных ситуаций

Нештатные ситуации классифицируются в соответствии с оценками, представленными в таблице «Порядок действий при обнаружении нештатных ситуаций».

Таблица. Порядок действий при обнаружении нештатных ситуаций.

1. – Оценки нештатных ситуаций

Нештатная ситуация		**Оценка ситуации (раздел Инструкции)**
Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа		(2.2)
Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации	Несанкционированное копирование защищаемой информации	Обнаружился случившийся факт (2.2)
		Производится в текущий момент (2.3)
	Несанкционированное изменение защищаемой информации	Обнаружился случившийся факт (2.2)
		Производится в текущий момент (2.3)
	Подключение ТС к средствам и системам ОИ	Обнаружился случившийся факт (2.2)
		Производится в текущий момент

Несанкционированный доступ к защищаемой информации	Установка закладочных устройств	Обнаружение установленных(2.2)
		Устанавливаются в настоящий момент
	Маскировка под зарегистрированного пользователя	Внешним злоумышленником в текущий момент
		Внутренним злоумышленником, либо производилась в прошлом(2.2)
	Использование дефектов ПООИ	Внешним злоумышленником в текущий момент
		Внутренним злоумышленником, либо производилось в прошлом (2.2)
	Использование программных закладок	Внешним злоумышленником в текущий момент
		Внутренним злоумышленником, либо производилось в прошлом (2.2)
	Обнаружение Программных вирусов	
	Хищение носителя Защищаемой информации	(2.2)
	Нарушение функционирования ТС обработки информации злоумышленником	Производится в текущий момент
		Обнаружился случившийся факт
	Блокирование доступа к защищаемой информации путем перегрузки ТС обработки информации ложными заявками на ее обработку	Производится в текущий момент внешним злоумышленником
		Производится в текущий момент внутренним злоумышленником
		Обнаружился случившийся факт
Ошибки пользователей системы при эксплуатации программных средств, ТС, средств и систем защиты информации		Ошибка повлекла утерю или повреждение защищаемой информации
		Ошибка привела к нарушению работоспособности ТС и ПО
Дефекты, сбои, отказы, аварии ТС, программных Средств и систем ОИ		

Сбои, отказы и аварии систем обеспечения ОИ		(2.18)
Природные явления, стихийные бедствия	Несущие угрозу жизни человека	(2.19)
	Ненесущие угрозу жизни человека	(2.20)

2.2. Нештатные ситуации, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником.

При обнаружении нештатных ситуаций, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником, создается комиссия.

В первую очередь АИБ ИС предпринимаются действия по сбору и обеспечению сохранности улик незаметно для злоумышленника при нештатных ситуациях, связанных с:

- разглашением защищаемой информации;
- обнаружением несанкционированно скопированной или измененной защищаемой информации;
- обнаружением подключения ТС к средствам и системам ОИ;
- обнаружением закладочных устройств;
- маскировкой под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки в прошлом (как внутренним, так и внешним злоумышленником);
- использованием дефектов ПООИ внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);
- использованием программных закладок внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);
- хищением носителя защищаемой информации.

Комиссия, дополнительно к общему порядку действий (в соответствии с разделом 3), должна:

- если это возможно, определить организации, в которые произошла утечка защищаемой информации;
- определить –возможные контрмеры, призванные уменьшить ущерб от утечки информации;

2.3. Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней.

В случае обнаружения злоумышленника неправомерно копирующего, либо изменяющего защищаемую информацию выполняются следующие действия:

- **первоочередные действия**
- АИБИС прерывает несанкционированный процесс;
- АИБ ИС блокирует доступ к ИС ГБОУ и для злоумышленника;
- АИБИС совместно с ответственным за обеспечение безопасности обработки персональных данных ГБДОУ удаляют нарушителя от средств ИС;
- ответственным за обработку персональных данных совместно с АИБ ИС предпринимаются действия по сбору и обеспечению сохранности улик;
- **последующие действия**
- создается комиссия для расследования инцидента.

2.4. Подключение технических средств к средствам и системам ОИ в текущий момент времени

В случае обнаружения злоумышленника, производящего подключение к техническим средствам и системам ОИ в текущий момент времени, выполняются следующие действия:

- **первоочередные действия:**
  - АИБИС прерывает процесс работы нарушителя;
  - в случае если нарушитель – пользователь ИС, АИБ ИС блокирует доступ в ИС ГБДОУ для нарушителя.
- **последующие действия:**
  - создается комиссия для расследования инцидента;

2.5. Установка закладочных устройств злоумышленником в текущий момент времени.

В случае обнаружения злоумышленника, устанавливающего закладочные устройства, выполняются следующие действия:

- **первоочередные действия:**
  - АИБИС сообщает правоохранительным органам, принимает меры к установлению личности злоумышленника;
- **последующие действия:**
  - создается комиссия для расследования инцидента.

2.6. Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени.

В случае обнаружения внешнего злоумышленника маскирующегося под зарегистрированного пользователя выполняются следующие действия:

- **первоочередные действия:**
  - АИБ ИС блокирует доступ к ГБДОУ для злоумышленника;
- **последующие действия:**
  - создается комиссия для расследования инцидента.

2.7. Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени.

В случае обнаружения использования дефектов ПООИ внешним нарушителем в текущий момент времени выполняются следующие действия:

- **первоочередные действия:**
  - АИБИС блокирует доступ из внешних сетей к оборудованию, на котором используется уязвимое ПО;
- **последующие действия:**
  - создается комиссия для расследования инцидента.

2.8. Использование программных закладок внешним нарушителем в текущий момент времени

В случае обнаружения использования программной закладки внешним нарушителем в текущий момент времени выполняются следующие действия:

- **первоочередные действия:**
  - АИБ ИС блокирует доступ из внешних сетей к оборудованию, на котором установлена программная закладка;
- **последующие действия:**
  - АИБИС определяет возможный ущерб, нанесенный программной закладкой;
  - АИБ ИС проводит мероприятия по обнаружению внедренных программных закладок и их нейтрализации, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента;
  - составляется акт об инциденте.

2.9. Обнаружение программных вирусов.

В случае обнаружения программных вирусов выполняются действия

предусмотренные Инструкцией по антивирусной защите.

2.10. Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником.

В случае обнаружения злоумышленника нарушающего функционирование ТС обработки информации в текущий момент времени выполняются следующие действия:

 первоочередные действия:

– АИБ ИС принимает меры по немедленному удалению злоумышленника от средств вычислительной техники (СВТ);

3. В случае если злоумышленник является пользователем системы, АИБ ИС блокирует доступ к ИС ГБДОУ для злоумышленника;

 последующие действия:

– В случае наличия повреждений АИБИС определяет ущерб, нанесенный ТС и информации;

– АИБИС производит восстановление работоспособности системы;

– создается комиссия для расследования инцидента.

2.11. Обнаружение нарушения функционирования ТС обработки информации, произведенного злоумышленником.

В случае обнаружения нарушений в функционировании ТС обработки информации, выполняются следующие действия:

– АИБИС определяет возможный круг лиц, причастных к нарушению функционирования ТС, определяет объем повреждений техническим и информационным ресурсам;

– АИБИС производит восстановление работоспособности системы;

– создается комиссия для расследования инцидента.

2.12. Блокирование доступа к защищаемой информации путем перегрузки ТС обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени.

В случае обнаружения внешней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки ТС обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия:

 первоочередные действия:

– АИБИС выявляет источник ложных заявок;

– АИБ ИС вырабатывает решение по блокированию потока ложных заявок и реализует выбранное решение;

 последующие действия:

– АИБ ИС уведомляет провайдера, от которого идут ложные заявки, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента;

– АИБИС составляет акт об инциденте.

2.13. Блокирование доступа к защищаемой информации путем перегрузки ТС обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени.

В случае обнаружения внутренней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки ТС обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия:

– АИБИС выявляет источник ложных заявок и блокирует доступ к ИС;

– создается комиссия для расследования инцидента.

2.14. Блокировка доступа к защищаемой информации, произошедшая в прошлом.

При обнаружении факта блокировки доступа к защищаемой информации, произошедшей в прошлом, выполняются следующие действия:

– АИБИС выявляет источник ложных заявок;

– в случае если злоумышленник является внешним, АИБИС уведомляет провайдера, от которого идут ложные заявки, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента;

– в случае если злоумышленник является внешним, АИБ ИС составляет акт об инциденте;

– создается комиссия для расследования инцидента.

2.15. Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации.

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации, выполняются следующие действия:

 первоочередные действия:

– АИБИС проводит анализ и идентификацию причин инцидента;

– в случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции;

– АИБИС определяет ущерб, нанесенный нештатной ситуацией;

– АИБИС проводит мероприятия по восстановлению работоспособности системы и информации;

 последующие действия:

– проводится проверка знаний сотрудника, виновного в инциденте, а в случае необходимости его обучение;

– АИБ ИС составляет акт об инциденте, в случае необходимости выносит предложение руководителю ГБДОУ о применении дисциплинарной меры в отношении нарушителя.

2.16. Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО.

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО, выполняются следующие действия:

 первоочередные действия:

– АИБИС проводит анализ и идентификацию причин инцидента;

– в случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.

 последующие действия:

– АИБ ИС определяет ущерб, нанесенный нештатной ситуацией, восстанавливают работоспособность системы;

– АИБИС составляет акт об инциденте, в случае необходимости выносит предложение о применении дисциплинарной меры в отношении нарушителя;

– проводится проверка знаний сотрудника виновного в инциденте, а в случае необходимости его обучение.

2.17. Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ.

В случае возникновения дефектов, сбоев, отказов, аварий ТС и систем ОИ выполняются следующие действия:

 первоочередные действия:

– АИБИС выявляют возможные причины проявления дестабилизирующих факторов;

– в случае наличия злоумышленных действий выполняется порядок действий

в соответствии с Приложением 2;

 последующие действия:

– АИБИС восстанавливает работоспособность систем;

– в случае потери данных АИБ ИС по возможности проводится восстановление их из резервных копий;

– АИБИС производится составление акта.

2.18. Сбои, отказы и аварии систем обеспечения ОИ.

В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем выполняется следующая последовательность действий:

– в случае если наблюдается продолжительное отключение электропитания, АИБИС производится отключение ТС до момента истечения резервов системы бесперебойного питания;

– ответственным за материально-техническое обеспечение организуются работы по максимально быстрому восстановлению систем обеспечения;

– в случае потери защищаемых данных ответственный за обработку персональных данных по возможности проводится восстановление их из резервных копий;

– ответственным за обработку персональных данных и ответственным за материально-техническое обеспечение производится составление акта.

2.19. Природные явления, стихийные бедствия, несущие угрозу жизни человека.

В случае проявления стихийных бедствий и природных явлений, которые несут угрозу жизни человека, выполняются следующие действия:

– все сотрудники (начальники отделов в том числе) обязаны предпринять максимально возможные меры по обеспечению сохранности личных реквизитов защиты (например: металлические и/или электронные ключи, карты-идентификаторы, ключевые дискеты, печати и пр.)вовремя эвакуации;

– всем сотрудникам обеспечить выключение рабочих станций;

– АИБИС выключает серверы и сетевое оборудование;

– АИБИС принимает меры к эвакуации резервных копий с информацией.

Заместители руководителя ГБДОУ обязаны собрать и обеспечить максимальные меры по обеспечению сохранности реквизитов защиты (например: металлические и/или электронные ключи, карты-идентификаторы, ключевые дискеты, печати и пр.) тех сотрудников, которых на момент эвакуации нет на рабочем месте (болезнь, командировка, учеба, отпуск и т.д.).

Заместители руководителя ГБДОУ обязаны проконтролировать исполнение задач эвакуации, приняв соответствующие доклады от сотрудников о готовности к эвакуации, провести выборочную проверку готовности личных реквизитов защиты пользователя ИС к эвакуации.

2.20. Природные явления, стихийные бедствия, не несущие угрозу жизни человека

В случае проявления стихийных бедствий и природных явлений, которые не несут угрозу жизни и/или человека, выполняются следующие действия:

– сотрудники ГБДОУ выключают свои персональные компьютеры;

– АИБИС выключает серверы и сетевое оборудование;

– АИБИС принимает меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества;

– пользователями ИС принимаются меры по обеспечению сохранности личных реквизитов защиты (например: металлические и/или электронные ключи, карты-идентификаторы, ключевые дискеты, печати и пр.);

– в случае локальных пожаров и частичных затоплений ответственным за материально-техническое обеспечение организуются работы по ликвидации нештатной ситуации и ее последствий.

3. Проведение расследований

Для расследования опасных ситуаций в случаях, предусмотренных настоящей Инструкцией, создается комиссия. В состав комиссии должны входить:

– председатель (руководитель ГБДОУ);

– ответственный за обработку персональных данных;

– АИБИС;

– другие лица по решению председателя комиссии.

Деятельность комиссии должна по возможности происходить в режиме конфиденциальности.

– В общем случае комиссия проводит:

– анализ идентификацию причин инцидента, определение виновных;

– определение ущерба, нанесенного нештатной ситуацией;

– планирование мер для предотвращения повторения, нейтрализации последствий (если это возможно);

– анализ и сохранение доказательств, следов инцидента, улик и свидетельств;

– определение меры взыскания с виновного;

– взаимодействие, при необходимости с правоохранительными органами.

При сохранении улик, если есть возможность, АИБ ИС производится резервное копирование системной и защищаемой информации ТС, вовлеченных в инцидент.

По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются поясняющие материалы (копии экрана, распечатки журнала событий, и др.).

По результатам расследования администраторами организуются мероприятия по реализации предложенных комиссией мер для предотвращения либо уменьшения вероятности проявления, подобных инцидентов в дальнейшем.

При проведении расследований, кроме того, необходимо ответить на следующие вопросы:

– можно ли было предупредить нештатную ситуацию?

– вызвана ли она слабостью средств защиты и регистрации?

– это первая кризисная ситуация такого рода?

– достаточно ли имеющегося резерва?

– есть ли необходимость пересмотра системы защиты?

– есть ли необходимость пересмотра настоящей инструкции?

4. Ответственные за контроль выполнения инструкции

Ответственными за постоянный контроль выполнения требований данной Инструкции являются:

– АИБИС в части задач, возложенных на него настоящей Инструкцией;

– ответственный за обработку персональных данных в части общего контроля информационной безопасности;

– ответственный за материально-техническое обеспечение, в части задач, возложенных на него настоящей Инструкцией.

5. Порядок замещения ответственных лиц

В случае отсутствия кого-либо из ответственных лиц при нештатной ситуации (отпуск, болезнь и т.п.) производится их замещение в соответствии с последовательностями определенными ниже. Ответственное лицо замещает следующий идущий по списку сотрудник.

Ответственные за информационную безопасность и ИС:

1. АИБИС;
2. ответственный за обработку персональных данных.

6. Порядок пересмотра инструкции

6.1. Инструкция подлежит полному пересмотру при изменении и приоритетов угроз безопасности ИС ГБДОУ, кроме того, полный плановый пересмотр данного документа проводится регулярно, не реже одного раза в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ИС ГБДОУ.

6.2. Инструкция подлежит частичному пересмотру в следующих случаях:

– при изменении местоположения, состава и объема информационных ресурсов, подлежащих резервному копированию;

– при определении такой необходимости комиссией по результатам расследования нештатной ситуации;

– в целях повышения эффективности мероприятий определенных в настоящей инструкции;

– при изменении состава, обязанностей и полномочий должностных лиц, которые задействованы в мероприятиях настоящей Инструкции.

6.3. Полный пересмотр данного документа проводится АИБ ИС, ответственным за обработку персональных данных ГБДОУ с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИС ГБДОУ.

6.4. Частичный пересмотр данного документа проводится АИБ ИС. Частичный пересмотр должен проводиться регулярно, не реже одного раза в полгода. При этом могут быть добавлены, удалены или изменены приложения Инструкции с обязательным указанием оснований и внесенных изменений в листе регистрации изменений в Инструкции (Приложение 4) без переутверждения всей Инструкции.

Приложение1
К Инструкции о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций

СРЕДСТВА ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ

Резервному копированию (РК) подлежит следующая информация:

- системные программы и наборы данных *–не возобновляемому (однократному, эталонному)РК*;
- прикладное программное обеспечение и наборы данных- *не возобновляемому РК*;
- наборы данных, генерируемые в течение рабочего дня и содержащие ценную информацию (журналы транзакций, системный журнал и т.д.) - *периодическому возобновляемому РК*.

Резервному копированию в ИС подлежат следующие программные информационные ресурсы:

Наименование информационного ресурса	**Где размещается ресурс в системе**	**Вид резервного копирования**	**Ответственный за резервное копирование (используемые технические средства)**	**Где хранится резервная копия**	**Частота периодического резервирования**
Информация ИС		Периодическое, возобновляемое	Администратор ИБИС		Ежедневно
Эталонное программное обеспечение		Не возобновляемое	Администратор ИБИС		Обновляется при появлении нового ПО

Приложение 2

К Инструкции о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций

План обеспечения непрерывной работы и восстановления информации

Тип кризисной ситуации	Критерии кризисной ситуации	Кому и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В не рабочее время		
Неправомерные действия со стороны лиц допущенных к защищаемой информации					
Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение несанкционированно скопированной или измененной конфиденциальной информации		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента	10 минут в рабочее время (1час в не рабочее)	
Несанкционированный доступ к информации					
Обнаружение подключения технических средств к средствам и системам объекта информатизации		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБ ИС как можно скорее, в дневное время, но не Позднее 8 часов после инцидента		
Подключение технических средств к Средствам и системам ОИ в текущий момент времени		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента	10минутв рабочее время (1часвнерабочее)	

Обнаружение закладочных устройств		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБ ИС как можно скорее, в дневное время, но не Позднее 8 часов после инцидента		
Установка закладочных устройств злоумышленником в текущий момент времени		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента	10минутв рабочее время (1час вне рабочее)	
Маскировка под зарегистрированного пользователя внешним злоумышленником в Текущий момент времени		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента	5минутв рабочее время (1час вне рабочее)	
Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не Позднее 8 часов после инцидента		
Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента	10минут в рабочее время (1час вне рабочее)	
Использование программных закладок внешним нарушителем в текущий момент времени		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента	10 минут в рабочее время (1час вне рабочее)	

Использование программных закладок внутренним злоумышленником или обнаружение факта использования		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение программных вирусов		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБ ИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента		12 часов
Хищение носителя защищаемой информации		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБ ИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента	10 минут в рабочее время (1час вне рабочее)	2 дня
	Нарушена работа группы пользователей	Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента	10 минут в рабочее время (1час вне рабочее)	1день
Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя	Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента		2 дня
	Нарушена работа группы	А Администратору ИБИС сразу после	Администратору ИБИС сразу после		1день

	пользователей	обнаружения инцидента	обнаружения инцидента		
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку					
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными Заявками на ее обработку внешним злоумышленником в текущий момент времени		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1час вне рабочее)	7 дней
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним Злоумышленником в текущий момент времени		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1час вне рабочее)	1день
Обнаружение произошедшего факта блокировки доступа к защищаемой информации		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не Позднее 8 часов после инцидента		1день
Ошибки пользователей системы					
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемо йинформации		Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов вне рабочее)	1день
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации,повлекшие нарушение работоспособности ТСИ ПО	Нарушена работа Одного пользователя	Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС в первый рабочий день после инцидента	20минут	2 дня
	Нарушена работа группы пользователей	Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС сразу после обнаружения инцидента	20минут	1день

Объективные факторы					
	Отказ ТС и систем ОИ, затронувший работу группы пользователей	Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час в рабочее время (8 часов вне рабочее)	1день
	Отказ ТС и систем ОИ, затронувший работу одного пользователя	Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБИС в первый рабочий день после инцидента	1 час	2 дня
	Авария ТС и систем ОИ	Администратору ИБИС сразу после обнаружения инцидента	Администратору ИБ ИС как можно скорее, в дневное время, но не Позднее 8 часов после инцидента	1 час	1день
Сбои, отказы и аварии систем обеспечения ОИ	Сбой систем Обеспечения ОИ	Ответственному за материально-техническое обеспечение сразу После инцидента	Ответственному за материально-техническое обеспечение в первый Рабочий день после инцидента		
	Отказ и систем обеспечения ОИ, затронувший работу группы пользователей	Ответственному за материально-техническое обеспечение и Администратору ИБ ИС сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение и Администратору ИБИС сразу после обнаружения инцидента		1день
	Отказ систем Обеспечения ОИ, затронувший работу одного пользователя	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническоеобеспечениев первыйрабочийденьпосле инцидента		2 дня

	Авария систем обеспечения ОИ	Ответственному за материально-техническое обеспечение, Администратору ИБИС сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение, Администратору ИБИС как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1день
Природные явления, стихийные бедствия, несущие угрозу жизни человека		Заместитель руководителя ГБДОУ, которые оповещают всех своих сотрудников сразу после получения информации	Заместитель руководителя ГБДОУ, которые оповещают Всех своих сотрудников сразу после получения информации		30минут
Природные явления, стихийные бедствия, ненесущие угрозу жизни человека		Заместитель руководителя ГБДОУ, Администратору ИБИС	Заместитель руководителя ГБДОУ, Администратору ИБИС		30минут

Приложение3
К Инструкции о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение4
К Инструкции о действиях лиц, допущенных к информации, содержащей персональные данные, в случае возникновения нештатных ситуаций

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Фамилия, инициалы сотрудника	Должность	Дата ознакомления	Расписка сотрудника в ознакомлении