19

Департамент социальной политики и занятости населения Брянской области
Государственное бюджетное стационарное учреждение социального обслуживания населения Брянской области
«Дятьковский дом-интернат для престарелых и инвалидов»»

ПРИКАЗ

От 13.06.2024 **№60** **п.Бытошь**

Об организации работы
с инцидентами информационной
безопасности

В целях исполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», анализа произошедших инцидентов информационной безопасности (далее – инцидентов), определения источников и причин возникновения инцидентов, оценки их последствий, планирования и принятия мер по предотвращению повторного возникновения инцидентов

ПРИКАЗЫВАЮ:

1. Создать постоянно действующую комиссию ГБСУСОН «Дятьковский дом-интернат для престарелых и инвалидов» (далее – Учреждение), по работе с инцидентами в составе (далее – комиссия):

Председатель комиссии: директор Киселев Сергей Иванович (ответственный за организацию обработки персональных данных);

Члены комиссии:

- главный бухгалтер Харитонова Тамара Николаевна (ответственный за обеспечение безопасности персональных данных в ИС);
- специалист по социальной работе Мамкова Екатерина Александровна
- специалист по социальной работе Киселёва Елена Ивановна
- медицинская сестра Карлинская Ольга Владимировна

2. Утвердить «Положение по работе с инцидентами информационной безопасности в ГБСУСОН «Дятьковский дом-интернат для престарелых и инвалидов» (Приложение 1).

3. Комиссии руководствоваться данным Положением при работе с инцидентами.

4. Уполномочить председателя комиссии при необходимости привлекать к работе комиссии других сотрудников ГБСУСОН «Дятьковский дом-интернат для престарелых и инвалидов», выступать с инициативой о привлечении

третьих лиц, не являющихся сотрудниками Учреждения, к работе с комиссией.

5. Утвердить форму журнала регистрации инцидентов информационной безопасности (Приложение 2).

6. Назначить ответственным за ведение и сохранность журнала регистрации инцидентов информационной безопасности специалиста по социальной работе Киселёву Елену Ивановну.

7. Хранить журнал в течение 5 лет после завершения его ведения.

8. Контроль за исполнением настоящего приказа оставляю за собой.

Директор С.И.Киселев

Ознакомлен

Харитонова Г.Н.

Маликова С.А.

Киселёва Е.И.

Карпинская О.К.

Приложение 1
к приказу ГБСУСОН
«Дятьковский дом-интернат для
престарелых и инвалидов»
от 13.06.2024 № 60

ПОЛОЖЕНИЕ
по работе с инцидентами информационной безопасности в ГБСУСОН «Дятьковский дом-интернат для престарелых и инвалидов»

Настоящее Положение разработано в целях организации работы с инцидентами информационной безопасности в ГБСУСОН «Дятьковский дом-интернат для престарелых и инвалидов» (далее – Учреждение).

1. Общие положения

Положение о работе с инцидентами информационной безопасности (далее – Положение) разработано в соответствии с:

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

требованиями по реализации мер, предусмотренных составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждёнными приказом ФСТЭК России от 18.02.2013 № 21;

правилами обработки персональных данных в Учреждении.

Инцидент - одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы (далее - ИС) и (или) к возникновению угроз безопасности информации, в том числе персональных данных.

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов и информационных систем.

Работа с инцидентами включает в себя следующие направления:

1) определение лиц, ответственных за выявление инцидентов и реагирование на них;

2) обнаружение, идентификация и регистрация инцидентов;

3) своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в

информационной системе пользователями и администраторами;

4) анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценка их последствий;

5) принятие мер по устранению последствий инцидентов;

6) планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий; планирования и принятия мер по предотвращению повторного возникновения инцидентов, назначается постоянно действующая комиссия по работе с инцидентами в соответствии с приказом руководителя Учреждения.

2. Сотрудники, ответственные за выявление инцидентов и реагирование на них.

2.1. Ответственными за выявление инцидентов являются:

сотрудники, имеющие право доступа к ИС и/или право доступа в кабинет, в котором произошел инцидент;

администратор ИС;

сотрудник, ответственный за обеспечение безопасности персональных данных в ИС.

2.2. Ответственными за реагирование на инциденты в ИС являются:

сотрудники, имеющие право доступа к ИС и/или право доступа в кабинет, в котором произошел инцидент;

администратор ИС;

ответственный за обеспечение безопасности персональных данных в ИС;

сотрудник, ответственный за организацию обработки персональных данных;

председатель комиссии по работе с инцидентами.

3. Обнаружение, идентификация и регистрация инцидентов

3.1. Работа по обнаружению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

выявление инцидентов в области информационной безопасности с помощью технических средств;

выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

выявление инцидентов с помощью сотрудников Учреждения.

3.2. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до сотрудников Учреждения информации, позволяющей идентифицировать инциденты.

Форма журнала утверждается приказом руководителя Учреждения.

Хранение журнала осуществляется в местах, исключающих доступ к

журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за ведение и хранение журнала назначается приказом директора Учреждения.

4. Информирование о возникновении инцидентов

Сотрудник Учреждения, обнаруживший инцидент, должен незамедлительно сообщить об инциденте сотруднику, ответственному за обеспечение безопасности персональных данных в ИС; ответственному за организацию обработки персональных данных; председателю комиссии по работе с инцидентами.

Сотрудник, ответственный за обеспечение безопасности персональных данных в ИС или председатель комиссии по работе с инцидентами, в случае необходимости, информирует пользователей ИС и прочих сотрудников Учреждения о возникновении инцидента и дает указания по дальнейшим действиям.

5. Анализ инцидентов, а также оценка их последствий

Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий осуществляет комиссия по работе с инцидентами информационной безопасности.

5.1. Источниками и причинами возникновения инцидентов в области информационной безопасности являются:

действия организаций и отдельных лиц враждебные интересам Учреждения;

отсутствие персональной ответственности сотрудников Учреждения обеспечение информационной безопасности, в том числе персональных данных;

недостатки в работе ответственных сотрудников по обеспечению необходимого режима соблюдения конфиденциальности в Учреждении, в том числе персональных данных;

недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;

совмещение функций по работе в информационной системе и с персональными данными с прочими функциями и обязанностями;

наличие избыточных привилегированных полномочий у пользователей в информационной системе;

пренебрежение сотрудниками Учреждения правил и требований по соблюдению информационной безопасности;

другие причины.

5.2. Оценка последствий инцидента производится комиссией по работе с инцидентами на основании выявления фактического или потенциально возможного ущерба.

6. Принятие мер по устранению последствий инцидентов

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

определение причин и последствий инцидента, ущерба причиненного инцидентом;

ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. Планирование и принятие мер по предотвращению инцидентов

7.1. Планирование и принятие мер по предотвращению возникновения инцидентов осуществляет комиссия по работе с инцидентами информационной безопасности и основывается на:

планомерной деятельности по повышению уровня знания сотрудников Учреждения правил и порядка информационной безопасности;

проведении обучения сотрудников Учреждения правилам и способам работы со средствами защиты информационных систем;

доведении до сотрудников требований законодательства, внутренних документов Учреждения, устанавливающих ответственность за нарушение требований информационной безопасности;

поддержание в актуальном, рабочем состоянии системы обеспечения информационной безопасности, с учетом возникновения новых угроз информационной безопасности и/или в случаях изменения требований законодательства и руководящих документов регуляторов по организации обеспечения информационной безопасности;

своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом.

Как правило, самым слабым звеном в любой системе безопасности является человек. Поэтому работа с персоналом является основным направлением деятельности по обеспечению требований информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Персонал Учреждения является основным источником сведений о возможных и произошедших инцидентах информационной безопасности. Оперативное информирование персоналом об инциденте информационной безопасности ответственных сотрудников Учреждения позволяют снизить ущерб от инцидента и являются основанием для смягчения либо отмены наказания сотрудников за нарушение требований информационной безопасности.

Приложение 2
к приказу ГБСУСОН «Дятьковский дом-интернат для престарелых и инвалидов»
от 13.06.2024 № 60

ЖУРНАЛ
регистрации инцидентов информационной безопасности
ГБСУСОН «Дятьковский дом-интернат для престарелых и инвалидов»

№ п/п	ФИО, должность, сотрудника обнаружившего инцидент	Дата выявления инцидента	Описание инцидента	Принятые меры по устранению последствий инцидента	Причины возникновения инцидента	Размер потенциально-возможного ущерба	Размер фактического ущерба	Принятые меры по предотвращению повторного возникновения инцидента
1	2	3	4	5	6	7	8	9
1								
2								
3								
4								
5								
6								
7								
8								