УТВЕРЖДЕНО
приказом директора
ГБУ КЦСОН Дубровского района
от 23.11.2018 г. № 85

Инструкция
по управлению инцидентами безопасности
в информационной системе
Государственного бюджетного учреждения Брянской области
«Комплексный центр социального обслуживания населения
Дубровского района»

1. Общие положения

1.1.Настоящий Инструкция по управлению инцидентами безопасности в информационной системе Государственного бюджетного учреждения Брянской области «Комплексный центр социального обслуживания населения Дубровского района» (далее – Инструкция) разработана в соответствии со ст. 18.1 и ст. 19 Федерального закона № 152-ФЗ «О персональных данных» и определяет порядок регистрации событий безопасности и порядок реагирования на выявленные инциденты безопасности, связанные с функционированием информационной системы персональных данных (далее - ПДн) Государственного бюджетного учреждения Брянской области «Комплексный центр социального обслуживания населения Дубровского района» (далее – ИС), а также меры и средства поддержания непрерывности работы и восстановления работоспособности ИС после инцидентов безопасности.

1.2.Задачами данной Инструкции являются:

- обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИС;
- установление процедур, направленных на предотвращение и выявление нарушений законодательства РФ в области защиты ПДн, а также устранение последствий таких нарушений;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер.

1.3.В Государственном бюджетном учреждении Брянской области «Комплексный центр социального обслуживания населения Дубровского района» (далее – Учреждение) ответственными за реагирование на инциденты безопасности являются администратор безопасности ПДн и Ответственный за обеспечение безопасности ПДн, назначаемые приказом директора Учреждения.

1.4.Действие настоящей Инструкции распространяется на всех работников Учреждения, имеющих доступ к ресурсам ИС.

2. Регистрация событий безопасности

2.1.События безопасности, подлежащие регистрации:

2.1.1. Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы.

2.1.2. Подключение машинных носителей информации и вывод информации на носители информации.

2.1.3. Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации.

2.1.4. Попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа.

2.1.5. Попытки удаленного доступа.

2.1.6. События, связанные с резервным копированием информации на резервные машинные носители информации.

2.1.7. События, связанные с восстановлением информации с резервных машинных носителей информации.

2.1.8. Запуск (завершение) работы компонентов виртуальной инфраструктуры.

2.1.9. Доступ субъектов доступа к компонентам виртуальной инфраструктуры.

2.1.10. Изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения.

2.1.11. Изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

2.2.Срок хранения событий безопасности – не менее 6 месяцев.

2.3.Ответственным за настройку параметров регистрации событий является администратор ИС. Настройка параметров регистрации событий осуществляется в следующих случаях:

- при вводе ИС в эксплуатацию;
- при изменении конфигурации ИС;
- при пересмотре перечня событий безопасности, подлежащих регистрации.

2.4.Состав и содержание информации о событиях безопасности:

2.4.1. При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2.4.2. При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного

носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

2.4.3. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

2.4.4. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

2.4.5. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

2.4.6. При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

2.4.7. При регистрации событий, связанных с резервным копированием информации на резервные машинные носители информации, а также связанных с восстановлением информации с резервных машинных носителей информации, состав и содержание информации должны включать дату, время события и идентификатор субъекта доступа и (или) иную информацию о событии.

2.4.8. При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры.

2.4.9. При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры.

2.4.10. При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период её аппаратного отключения состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры.

2.4.11. При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры.

2.5. Порядок обработки информации о событиях безопасности:

2.5.1. Реагирование на сбои, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти, при регистрации событий безопасности предусматривает:

- предупреждение (сигнализация, индикация) администратора ИС о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

- реагирование на сбои при регистрации событий безопасности путем изменения администратором ИС параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

2.5.2. Мониторинг (просмотр и анализ) записей регистрации событий безопасности проводится администратором ИС для всех событий, подлежащих регистрации.

2.5.3. В случае выявления признаков инцидентов безопасности в ИС администратор ИС вносит сведения об инцидентах безопасности в «Журнал учета инцидентов безопасности» (Приложение 1), осуществляет планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности. Обязательной фиксации подлежит следующая информация об инциденте безопасности:

- дата и время регистрации в ИС инцидента безопасности;
- описание инцидента безопасности;
- уровень критичности инцидента в соответствии с приведенной в разделе 3 настоящей Инструкции классификацией;
- последствия: нарушение конфиденциальности/целостности/доступности ПДн, величина нанесенного ущерба (если он есть);
- действия, предпринятые для устранения результатов последствий;
- результаты расследования, проведенного в соответствии с разделом 4 настоящей Инструкции.

2.5.4. Ведение «Журнала учета инцидентов безопасности» может осуществляться в электронном или бумажном виде.

3. Реагирование на выявленные инциденты безопасности

3.1.1. Все работники Учреждения обязаны немедленно уведомлять непосредственных руководителей и ответственных за реагирование на инциденты безопасности о случаях нарушения защиты или об обнаруженных уязвимостях в информационных системах и средствах защиты.

3.1.2. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники Учреждения предпринимают меры по восстановлению работоспособности. Предпринимаемые меры должны согласовываться с вышестоящим руководством, но в случаях, требующих оперативных мер, допускается действовать без согласования. При необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3.1.3. При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

<u>Уровень 1:</u>

Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность/конфиденциальность/целостность элементов ИС и средств защиты. Эти инциденты решаются ответственными за реагирование работниками.

Уровень 2:

Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИС и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование работниками и решаются с привлечением Администратора ИС.

Уровень 3:

Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИС и средств защиты, а также к угрозе жизни пользователей ИС, классифицируется, как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к нарушению работоспособности ИС и средств защиты на сутки и более:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки в непосредственной близости от зданий офисов Учреждения.

4. Расследование инцидентов, связанных с нарушениями защиты ПДн

4.1.По каждому инциденту, связанному с нарушением защиты ПДн в Учреждении, должно проводиться расследование. Ответственность за проведение расследования возлагается на Администратора ИС и Ответственного за обеспечение безопасности ПДн. Руководители структурных подразделений, в которых произошел инцидент, и находящиеся в их подчинении сотрудники обязаны оказывать содействие в сборе необходимой для расследования информации и в устранении последствий инцидента.

4.2. В результате расследования необходимо определить:

- нарушителя (нарушителей) защиты ПДн;
- тип нарушения и величину нанесенного ущерба (если он есть);
- причины, приведшие к нарушению;
- меры и средства, необходимые для ликвидации нежелательных последствий;
- меры и средства, необходимые для ликвидации или ослабления причин, приведших к нарушению, чтобы подобные нарушения не повторялись в будущем.

4.3.Результаты расследования должны оформляться документально.

5. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

5.1.Технические меры.

5.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные и аппаратные средства и системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, такие как:

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

5.1.2. Системы жизнеобеспечения ИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

5.1.3. Все помещения Учреждения (помещения, в которых размещаются элементы ИС и средства защиты) должны быть оборудованы средствами пожарной сигнализации. Доступ в эти помещения посторонних лиц ограничен в нерабочее время.

5.2.Организационные меры.

5.2.1. Ответственные за реагирование работники знакомят всех работников Учреждения, находящихся в их зоне ответственности, с данной Инструкцией. Новые работники должны быть ознакомлены с данной Инструкцией в срок, не превышающий трех рабочих дней с момента выхода нового работника на работу.

5.2.2. Навыки и знания работников Учреждения по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение работников Учреждения порядку действий при возникновении аварийной ситуации.

6. Ответственность за нарушение требований обеспечения защиты ПДн

6.1.Ответственность за нарушение требований обеспечения защиты ПДн накладывается на работников Учреждения, совершивших нарушения, в зависимости от типа нарушения, возникшего в результате необеспечения или нарушения защиты ПДн, и величины причиненного ущерба (нежелательных последствий).

6.2.Работники Учреждения могут привлекаться к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации и административно-правовыми нормами, установленными в Учреждении.

С инструкцией ознакомлен (а):

№ п/п	Должность	ФИО	Дата ознакомления	Подпись

Административно-управленческий персонал				
1.	Директор	Трифонова Н.В.		
2.	Зам. Директора	Савченков А.Е.		
3.	Зам. Директора	Лескина Н.Б.		
4.	Врач – заведующий медицинским кабинетовё	Чубыкин В.Я.		
5.	Главный бухгалтер	Сивачева Н.А.		
6.	Ведущий бухгалтер	Сергеенкова С.П.		
7.	Бухгалтер 1 категории	Сидукина Н.А.		
8.	Специалист по кадрам	Попова Л.И.		
Стационарное отделение временного проживания граждан пожилого возраста и инвалидов				
1.	Специалист по социальной работе	Башурина И.В.		
2.	Медицинские сестры	Фролова В.В.		
		Удалых Е.В.		
Отделение социально – медицинского обслуживания на дому граждан пожилого возраста и инвалидов				
1.	Заведующий отделением	Соломникова И.Г.		
2.	Социальные работники	Аташева Е.И.		
		Рябушева Е.В.		
		Прядехина Н.А.		
		Функова В.В.		
		Филина Е.И.		
Отделение срочного социального обслуживания и консультативной помощи				
1.	Специалист по социальной работе	Лапутина В.А.		
Отделение дневного пребывания и реабилитации				
1.	Заведующий отделением	Петрушина Л.П.		
2.	Психолог	Василенкова Т.А.		
3.	Логопед	Полукова Н.А.		
4.	Специалист по социальной работе	Митрошина Г.А.		
Отделение помощи семье, женщинам и детям со стационаром				
1.	Педагог-психолог	Мартынова О.В.		
2.	Социальный педагог	Крючкова Е.А.		
3.	Специалист по социальной работе	Логвинова В.И.		
4.	Медицинская сестра	Терехова Е.В.		
5.	Воспитатели	Морозова В.И.		
		Буравилина Г.А.		
		Кострюкова Н.А.		
		Болобонова Е.Н.		
		Горбунова Е.Н.		
		Мамичева Е.В.		

Приложение 1
к Инструкции по управлению
инцидентами безопасности
в информационной системе
ГБУ КЦСОН Дубровского района

ЖУРНАЛ
УЧЕТА ИНЦИДЕНТОВ
БЕЗОПАСНОСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
БРЯНСКОЙ ОБЛАСТИ
«КОМПЛЕКСНЫЙ ЦЕНТР СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ
НАСЕЛЕНИЯ ДУБРОВСКОГО РАЙОНА»

(НАИМЕНОВАНИЕ УЧРЕЖДЕНИЯ С УКАЗАНИЕМ ПРАВОВОЙ ФОРМЫ)

242750, Брянская область, Дубровский район, пгт. Дубровка, 1-ый микрорайон, д. 1

тел. 8(48332)9-11-99

(МЕСТО РАСПОЛОЖЕНИЯ УЧРЕЖДЕНИЯ)

Начат _____

Окончен _____

№ п/п	ФИО, должность, структурное подразделение работника обнаружившего инцидент	Дата выявления инцидента	Описание инцидента	Принятые меры по устранению последствий инцидента	Причины возникновения инцидента	Причиненный ущерб	Принятые меры по предотвращению повторного возникновения инцидента
1	2	3	4	5	6	7	9