УТВЕРЖДЕН

приказом директора
ОГБУ «КЦСО ЕАО»
от «02» 07 2024 г. № 184

ПОРЯДОК РЕАГИРОВАНИЯ
на инциденты при обработке персональных данных в ИСПДн областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области»

1. Общие сведения

1.1 Настоящий документ определяет порядок действий в случае обнаружения инцидентов информационной безопасности при обработке конфиденциальной информации, в том числе персональных данных в ОГБУ «КЦСО ЕАО» (далее – Учреждение).

1.2 К инцидентам информационной безопасности при обработке конфиденциальной информации, в том числе персональных данных (далее – инциденты ИБ) относятся:

- нарушение конфиденциальности, целостности или доступности конфиденциальной информации, в том числе персональных данных;
- отказ оборудования, сервисов, средств обработки и (или) защиты информации;
- несоблюдение требований внутренней организационно-распорядительной документации и действующего законодательства Российской Федерации в области защиты информации;
- заражение вредоносными программами.

К инцидентам информационной безопасности также относятся попытки и факты получения несанкционированного доступа к информационным системам персональных данных (ИСПДн):

- сеансы работы в ИСПДн незарегистрированных пользователей;
- сеансы работы Пользователей ИСПДн, срок действия полномочий которых истёк, либо в состав полномочий которых не входит обработка персональных данных;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учётной записи другого пользователя в целях получения коммерческой или другой личной выгоды методом подбора пароля

или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учётной записи;

- совершение попыток несанкционированного доступа к АРМ, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);

- несанкционированное внесение изменений в конфигурации программных или аппаратных средств обработки или защиты персональных данных.

Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для наступления случаев, описанных выше.

1.3 В соответствии с частью 3.1 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в случае выявления инцидента Учреждение обязано уведомить уполномоченный орган по защите прав субъектов персональных данных – Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

1.4 В соответствии с частью 12 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» Учреждение обязано в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ России), обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

2. Порядок реагирования на инциденты информационной безопасности

2.1. Последовательность действий работника в случае выявления инцидента ИБ:

- прекратить работу с ресурсом, в котором выявлен инцидент ИБ;

- оповестить непосредственного руководителя о факте выявления инцидента ИБ;

- непосредственный руководитель работника должен оповестить ответственного за организацию обработки персональных данных о факте выявления инцидента ИБ;

- ответственный за организацию обработки персональных данных и администратор информационной безопасности (далее – администратор ИБ) собирают всю необходимую информацию для анализа инцидента ИБ.

2.2. Ответственный за организацию обработки персональных данных проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его наступлению, и составляет краткую справку, в которой описываются произошедший инцидент ИБ, его последствия (при наличии) и оценка необходимости проведения расследования инцидента ИБ, возможные меры для устранения последствий инцидента.

3. Порядок действий в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных

3.1. В случае если инцидент ИБ может стать (или уже стал) причиной негативных последствий для субъектов персональных данных, необходимо немедленно прекратить обработку персональных данных этих субъектов и по возможности блокировать доступ к этим данным до устранения причин, повлекших наступление инцидента ИБ и его последствий. Решение о блокировании доступа к персональным данным принимает ответственный за организацию обработки персональных данных. Производится анализ ситуации и реализуются оперативные контрмеры, которые можно применить для локализации инцидента.

3.2. Ответственный за организацию обработки персональных данных в Учреждении уведомляет субъекта персональных данных об инциденте и принятых мерах блокирования доступа к его персональным данным.

3.3. Ответственный за организацию обработки персональных данных обязан уведомить Роскомнадзор в течение 24 (двадцати четырех) часов о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента.

Ответственное лицо должно подать уведомление о данном инциденте на сайте Роскомнадзора (https://pd.rkn.gov.ru/incidents/), пройдя верификацию через сервис ЕСИА.

3.4. Персональные данные остаются заблокированными до устранения причин, повлекших наступление инцидента ИБ. Если причины возникновения инцидента ИБ невозможно устранить, то персональные данные должны быть уничтожены. Ответственный за организацию обработки персональных данных и

администратор ИБ обеспечивают немедленное уничтожение персональных данных.

3.5. Ответственный за организацию обработки персональных данных оповещает субъекта персональных данных о прекращении обработки и уничтожении его персональных данных.

3.6. В порядке, определённом нормативными документами ФСБ России, необходимо обеспечить взаимодействие с ГосСОПКА и передать информацию об инцидентах ИБ, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных, в Национальный координационный центр по компьютерным инцидентам (НКЦКИ). В случае возникновения инцидента в НКЦКИ должна быть направлена следующая информация:

– дата, время, место происшествия;

– наличие связи между инцидентом и компьютерной атакой;

– связь с другими происшествиями – при наличии;

– технические параметры компьютерного инцидента;

– последствия.

Передать информацию об инциденте возможно через техническое подключение к ГосСОПКА или путём отправки информации по E-mail, телефону, факсу на контакты НКЦКИ, указанные на их сайте http://cert.gov.ru. Срок передачи информации об инциденте ИБ – 24 часа с момента происшествия.

4. Порядок расследования инцидента

4.1. Разбирательство и составление заключений в обязательном порядке должны проводиться в случае выявления следующих фактов:

- нарушение конфиденциальности, целостности, доступности персональных данных;

- халатность и несоблюдение требований по обеспечению безопасности персональных данных;

- несоблюдение условий хранения носителей персональных данных;

- использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

4.2. В случае установления неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, ответственный за организацию обработки персональных данных обязан уведомить Роскомнадзор в течение 72 (семидесяти двух) часов о результатах внутреннего

расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Ответственный за организацию обработки персональных данных должен подать уведомление о результатах внутреннего расследования на сайте Роскомнадзора (https://pd.rkn.gov.ru/incidents/), пройдя верификацию через сервис ЕСИА.

4.3. Проведение внутреннего расследования инцидента возлагается на комиссию, в состав которой должны входить администратор ИБ, ответственный за организацию обработки персональных данных, специалист по технической поддержке, лица, сообщившие об инциденте и другие лица, имеющие отношение к данному инциденту.

Задачами внутреннего расследования являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

- установление лиц, непосредственно виновных в данном нарушении;

- выявление причин и условий, способствовавших нарушению.

Права и обязанности комиссии:

- опрос работников, допустивших нарушение конфиденциальности информации, а также лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента ИБ;

- проведение осмотров объектов и предметов, которые могут иметь отношение к факту нарушения;

- привлечение (с разрешения соответствующего руководителя) других работников к проведению отдельных действий в рамках внутреннего расследования.

Все действия членов комиссии и полученные в ходе расследования материалы подлежат письменному оформлению. В целях исключения возможности какого-либо воздействия на процесс расследования члены комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения главным врачом Учреждения.

Для организованного и оперативного проведения внутреннего расследования администратор ИБ разрабатывает версии причин и составляет план проведения необходимых мероприятий по каждой из этих версий.

В ходе расследования могут выдвигаться и отрабатываться дополнительные версии, в этом случае план действий уточняется. Одновременно с проведением внутреннего расследования, директор Учреждения может поручить Комиссии определить актуальность утраченной (разглашённой) конфиденциальной информации, а также определить (подсчитать) ущерб (убытки) по расследуемому факту.

По окончании внутреннего расследования комиссия представляет директору Учреждения заключение, в котором излагаются:

- основания и время проведения расследования;
- проделанная работа (кратко);
- время, место и обстоятельства факта нарушения;
- причины и условия совершения нарушения;
- виновные лица и степень их вины;
- наличие умысла в действиях виновных лиц;
- предложения по возмещению ущерба;
- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;
- рекомендации по исключению подобных нарушений;
- другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т.д.). К заключению прилагаются:
- письменные объяснения лиц, которых опрашивали члены Комиссии;
- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т.д.;
- другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба (убытков).

Заключение должно быть подписано всеми членами комиссии. При несогласии с выводами или содержанием отдельных положений член комиссии, подписывая заключение, приобщает к нему своё особое мнение (в письменном виде). Заключение по результатам расследования подлежит утверждению директором Учреждения.

4.4. Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с заключением по результатам расследования. Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

При наличии в действиях лица признаков административного правонарушения или уголовного преступления директор Учреждения обязан обращаться в правоохранительные органы для привлечения виновного к ответственности в соответствии с законодательством Российской Федерации.

В соответствии с Трудовым кодексом возмещение ущерба проводится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчёта ущерба взыскание должно производиться по решению суда. В этом случае заключение

по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нарушение режима конфиденциальности.

Первый экземпляр заключения с резолюцией директора, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле.

Дело о внутренних расследованиях вносится в номенклатуру дел ОГБУ «КЦСО ЕАО».

5. Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение

5.1. Мероприятия, в зависимости от произошедшего инцидента ИБ, включают в себя:

- мониторинг событий в информационной системе персональных данных;
- восстановление операционной системы рабочей станции, на которой произошел инцидент ИБ, на заводские настройки;
- своевременное удаление неиспользуемых учётных записей;
- контроль и мониторинг действий пользователей в информационной системе персональных данных;
- контроль над действиями системного администратора;
- проведение обучения (повторного обучения) пользователей правилам обработки и защиты персональных данных;
- ознакомление пользователей с мерами ответственности, установленными законодательством Российской Федерации за нарушение норм и правил обработки персональных данных, а также за разглашение полученных данных;
- пересмотр организационно-распорядительной документации, устанавливающей правила обработки и обеспечения безопасности при работе с персональными данными.

6. Пересмотр и внесение изменений в организационные документы по обеспечению безопасности информации

6.1. Пересмотр положений настоящего и иных локальных документов ОГБУ «КЦСО ЕАО», касающихся вопросов обработки и обеспечения безопасности персональных данных, проводится в следующих случаях, если иное не установлено в пересматриваемых документах:

- при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти РФ;

- по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности персональных данных;

- по результатам внутреннего контроля (аудита) системы защиты персональных данных в случае выявления существенных нарушений;

- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности персональных данных и выявивших недостатки в правилах предоставления доступа к персональным данным.

6.2. Ответственным за пересмотр настоящего Регламента являются администратор информационной безопасности и ответственный за организацию обработки персональных данных. Внесение изменений производится на основании соответствующего приказа директора Учреждения.