Департамент социальной защиты населения Вологодской области

Бюджетное учреждение социального обслуживания Вологодской области
«Комплексный центр социального обслуживания населения
города Череповца и Череповецкого района «Забота»
(БУ СО ВО «КЦСОН «Забота»)

ПРИКАЗ

от 15.12.2021 № 364/01-05

Об утверждении Политики

В соответствии с Федеральным Законом «О персональных данных» от 27.07.2006 № 152-ФЗ
ПРИКАЗЫВАЮ:

Утвердить Политику информационной безопасности бюджетного учреждения социального обслуживания Вологодской области «Комплексный центр социального обслуживания населения города Череповца и Череповецкого района «Забота» (прилагается).

Директор С.Ю.Дуборова

УТВЕРЖДЕНО:
Приказом БУ СО ВО «КЦСОН «Забота»
от 15.12.2021 № 364/01-05

Политика информационной безопасности бюджетного учреждения социального обслуживания Вологодской области «Комплексный центр социального обслуживания населения города Череповца и Череповецкого района «Забота»
(далее – Политика)

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с положениями:
- Конституции Российской Федерации;
- Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федерального закона от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне";
- Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";
- Национального стандарта РФ ГОСТ Р ИСО/МЭК 27033-1-2011 "Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции", утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. N 683-ст);
- общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности.

1.2. Политика представляет собой совокупность положений, правил, требований и принятых решений, определяющих порядок доступа к информационным ресурсам бюджетного учреждения социального обслуживания Вологодской области «Комплексный центр социального обслуживания населения города Череповца и Череповецкого района «Забота» (далее – учреждение), основные направления и способы защиты информации.

1.3. Основными целями Политики являются:
- обеспечение управления и поддержки высшим руководством учреждения информационной безопасности в соответствии с соответствующими законами и нормами;
- защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба;
- обеспечение целостности и конфиденциальности информации;
- обеспечение соблюдения требований законодательства, руководящих и нормативных документов и общей политики безопасности.

1.4. Основными задачами Политики являются:
- доступность обрабатываемой информации;
- защита информации от несанкционированного доступа к ней посторонних лиц, от утечки по техническим каналам, от специальных воздействий на информацию в целях её блокирования, уничтожения, искажения;

- контроль целостности и аутентичности (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой по каналам связи учреждения;

- обеспечения конфиденциальности определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи учреждения;

- оценка рисков информационной безопасности.

1.5. Защите подлежит вся принимаемая, передаваемая, обрабатываемая и хранимая информация содержащая:

- персональные данные, доступ к которым ограничен в соответствии с положениями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";

- открытые сведения, в части обеспечения доступности и целостности информации.

1.6. Основными способами защиты информационных ресурсов являются:

- оценка рисков информационной безопасности;

- мониторинг событий безопасности;

- системный аудит;

- антивирусный контроль;

- анализ инцидентов.

1.7. Основными средствами защиты информационных ресурсов являются:

- средства криптографической защиты информации: ViPNet, КриптоПро, Континент;

- программные и программно-аппаратные комплексы межсетевого экранирования ViPNet;

- средства обеспечения антивирусной защиты и контроля целостности программных и информационных ресурсов: Dr.web, Лаборатория Касперского;

- средства идентификации и аутентификации пользователей: персональные логины и пароли;

- штатные средства разграничения прав доступа к информационным ресурсам и контроля событий безопасности, встроенные в применяемое программное обеспечение, включая программное обеспечение средств защиты информации.

1.8. Политика утверждается директором учреждения и доводится до сведения всех работников учреждения.

1.9. Основные положения и требования настоящей Политики распространяются на все структурные подразделения учреждения.

2. Субъекты правоотношений, связанных с использованием информации и обеспечением ее безопасности

2.1. К субъектам правоотношений, связанных с использованием информационных ресурсов учреждения и обеспечением их безопасности (далее - субъекты правоотношений) относятся:

- учреждение, как собственник информационных ресурсов;

- работники учреждения, обрабатывающие информацию в соответствии с возложенными на них трудовыми обязанностями;

- подразделения учреждения и обслуживающих организаций, обеспечивающие эксплуатацию информационных ресурсов;

- иные пользователи (физические и юридические лица), информация о которых обрабатывается, накапливается и хранится в учреждении (далее - пользователи).

2.2. В целях организации процесса использования информационных ресурсов учреждение обязано соблюдать следующие требования:

2.2.1. Назначение и распределение ролей должностных лиц структурных подразделений;

2.2.2. Обеспечение информационной безопасности компонентов информационно-телекоммуникационных сетей и информационных систем (далее соответственно – ИТС, ИС) на стадиях жизненного цикла;

2.2.3. Защита от несанкционированного доступа (далее - НСД), управления доступом и регистрацией действий в ИС;

2.2.4. Антивирусная защита;

2.2.5. Использование средств криптографической защиты информации;

2.2.6. Использование электронной подписи;

2.2.7. Защита персональных данных;

2.2.8. Защита основных компонентов ИТС, ИС.

2.3. Доступ к информационным ресурсам учреждения имеют работники, назначенные ответственными за организацию и (или) за обработку персональных данных в учреждении.

Уровень доступа к информационным ресурсам учреждения определяется для каждого работника индивидуально с соблюдением следующих требований:

- каждый работник имеет доступ только к той информации, которая необходима ему для выполнения должностных обязанностей;

- непосредственный руководитель работника имеет право на просмотр информации, используемой работником.

Все работники должны быть ознакомлены персонально под роспись с организационно-распорядительными документами по защите информации, должны знать и неукоснительно выполнять технологические инструкции и общие обязанности по обеспечению безопасности информации.

Каждый работник при приеме на работу подписывает обязательство о соблюдении требований по обеспечению конфиденциальности информации и ответственности за их нарушение, а также о выполнении правил работы с информацией.

Все работники, допущенные к обработке конфиденциальной информации несут персональную ответственность за нарушение правил ее использования, передачи, хранения, а также требований по обеспечению конфиденциальности информации.

3. Угрозы безопасности информации и их источники

3.1. Угрозы безопасности информации, с которыми сталкивается учреждение, могут быть связаны с проблемами:

- несанкционированного доступа к информации;
- несанкционированной передачи информации;
- воздействия вредоносной программы;
- отказа от факта приема и (или) передачи информации;
- отказа в обслуживании и недоступности информации или услуг.

3.2. Основными источниками угроз безопасности информации являются: нарушение конфиденциальности, целостности или доступности информации, возможность воздействия на компоненты ИТС и ИС, приводящего к их утрате, уничтожению или сбою функционирования.

4. Оценка рисков сетевой безопасности

4.1. Для идентификации и подтверждения технических мер и средств контроля и управления безопасностью информации в учреждении проводится оценка риска сетевой безопасности.

Для этого должны быть выполнены следующие основные действия:

- определение степени значимости информации, выраженной с точки зрения потенциального неблагоприятного воздействия на основную деятельность учреждения в случае возникновения нежелательных событий (инцидентов);

- идентификация и оценка вероятности или уровней угроз, направленных против информации;

- идентификация и оценка степени серьезности или уровня уязвимостей (слабых мест), которые могли бы быть использованы для реализации выявленных угроз;

- оценка величины рисков, основывающихся на определенных последствиях потенциального неблагоприятного воздействия на деятельность учреждения, уровнях угроз и уязвимостей.

5. Мониторинг информационной безопасности

5.1. Мониторинг работоспособности программных и программно-аппаратных компонентов ИТС и ИС, обрабатывающих информацию, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования.

Наиболее существенные компоненты систем(серверы, активное сетевое оборудование), должны оснащаться средствами контроля работоспособности, и контролироваться постоянно в процессе их эксплуатации.

5.2. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей;

- обнаружение дубликатов идентификаторов пользователей;- ежеквартальный контроль функционирования правил генерации паролей (обязательное использование установленных категорий символов, минимальная длинна, количество неуспешных попыток до блокировки учетной записи и т.д.).

5.3. Мониторинг целостности программного обеспечения включает следующие действия:

- проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;

- восстановление системных файлов администраторами систем с резервных копий в случае сбоев.

5.4. Мониторинг попыток несанкционированного доступа осуществляется с использованием штатных средств регистрации событий безопасности, встроенных в применяемое программное обеспечение, включая программное обеспечение средств защиты информации, и предусматривает:

- фиксацию неудачных попыток входа в систему и (или) повышения привилегий в системном журнале;

- протоколирование работы сетевых сервисов;

- выявление фактов злонамеренных программно-математических воздействий.

5.5. Мониторинг производительности автоматизированных систем, обрабатывающих информацию, производится по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления

попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

6. Антивирусный контроль

6.1. Для защиты сервера необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- утилиты для обнаружения и анализа новых вирусов.

6.2. К использованию допускаются только сертифицированные средства защиты от вредоносных программ и вирусов, лицензионные или свободно распространяемые.

6.3. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать альтернативные антивирусные средства в формате portable либо Live CD.

6.4. Установка и настройка средств защиты от вредоносных программ и вирусов на серверах ИТС и ИС, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке используемых средств защиты.

6.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

6.6. Антивирусный контроль должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

6.6. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флеш-накопителей и т. п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

6.7. Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

6.8. На всех рабочих станциях и серверах необходимо организовать регулярное обновление антивирусных баз.

6.9. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которые распространяются вирусы.

6.10. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т. д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

7. Анализ инцидентов

7.1. Если администратор системы, обрабатывающей информацию, подозревает или получил сообщение о том, что эта система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки несанкционированного доступа (НСД);
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точку входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

7.2. Для выявления попытки НСД необходимо:

- установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях;
- выявить подозрительную активность пользователей;
- проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго;
- проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

7.3. При анализе событий безопасности на автоматизированных рабочих местах и серверах администратору необходимо произвести следующие действия:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованных подозрительным абонентам;
- проверить системные журналы на предмет аномальных событий;
- выявить попытки повышения привилегий учетной записи пользователя;
- выявить наличие неудачных попыток входа в систему.

7.4. В ходе анализа журналов активного сетевого оборудования (маршрутизаторов, шлюзов) необходимо:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;
- проверить, не уничтожен ли системный журналполностью либо частично;
- проверить системные журналы на предмет аномальных событий;
- выявить попытки изменения таблиц маршрутизации и адресных таблиц;
- проверить конфигурацию сетевых устройств с целью выявления анализаторов трафика.

7.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- сопоставить конфигурацию системы с ее эталонной конфигурацией;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных файлов;
- проверить систему аутентификации и авторизации.

7.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

8. Особенности обеспечения безопасности персональных данных

8.1. В учреждении выделяются следующие категории персональных данных:

- биометрические персональные данные;
- общедоступные или обезличенные персональные данные.

8.2. К субъектам персональных данных относятся:

- работники учреждения;
- граждане, претендующие на замещение должностей в учреждении;
- члены семей лиц (близкие родственники) работников учреждения;
- лица, уволенные из учреждения;
- лица, которым осуществляется перечисление средств, удерживаемых у работников учреждения в соответствии с судебными решениями или их заявлениями, в том числе алиментов;
- лица, получающие социальные услуги в учреждении;
- лица, обратившиеся в учреждение за социальными услугами;
- лица, осуществляющие волонтерскую деятельность в учреждении;
- лица, направившие обращение в учреждение.

8.3. Все персональные сведения о субъекте персональных данных учреждение может получить только от него самого.

8.4. Учреждение обязано сообщить субъекту персональных данных о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа дать письменное согласие на их получение.

8.5. Персональные данные субъекта персональных данных являются конфиденциальной информацией и не могут быть использованы учреждением или любым иным лицом в личных целях.

8.6. При определении объема и содержания персональных данных учреждение руководствуется настоящей Политикой, Конституцией РФ, Федеральным законом 152-ФЗ «О персональных данных», иными федеральными

законами и принимаемыми в соответствии с ними нормативными правовыми актами.

8.7. Персональные данные хранятся в электронном виде, на бумажных носителях.

8.8. Право доступа к персональным данным имеют работники, назначенные ответственными за обработку персональных данных в учреждении.

8.9. Учреждение обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей по защите персональных данных, предусмотренных Федеральным законом 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Учреждение самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей по защите персональных данных, в соответствии с требованиями Федерального закона 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам относятся:

1) назначение ответственного за организацию обработки персональных данных;

2) издание документов, определяющих политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

6) ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

8.10. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных учреждение осуществляет блокирование неправомерно обрабатываемых персональных данных с момента такого обращения на период проверки.

8.11. В случае выявления неточных персональных данных при обращении субъекта персональных данных учреждение осуществляет блокирование персональных данных с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

8.12. В случае подтверждения факта неточности персональных данных учреждение на основании сведений, представленных субъектом персональных данных, или иных необходимых документов уточняет персональные данные в

течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

8.13. В случае выявления неправомерной обработки персональных данных, учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

8.14. В случае если обеспечить правомерность обработки персональных данных невозможно, учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

8.15. Об устранении допущенных нарушений или об уничтожении персональных данных учреждение уведомляет субъекта персональных данных.

8.16. В случае достижения цели обработки персональных данных учреждение прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

8.17. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных учреждение прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

8.18. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 9.13-9.16 настоящей Политики, учреждение осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8.19. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами.

8.20. Моральный и имущественный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

9. Заключительные положения

9.1. Настоящая Политика вступает в силу с момента ее утверждения.

9.2. Руководитель учреждения обеспечивает неограниченный доступ к настоящему документу.

9.3. Настоящая Политика доводится до сведения всех работников персонально под роспись.