Министерство социальной политики Красноярского края
КРАЕВОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«Централизованная бухгалтерия по ведению учета в сфере социальной поддержки и социального обслуживания граждан»
(КГКУ «ЦБ»)

ПРИКАЗ № 80/3-716

г. Красноярск «02» 09 2020 года

«Об утверждении Политики
информационной безопасности»

С целью обеспечения защиты прав субъектов персональных данных при получении, обработке, хранении и их передаче, руководствуясь Трудовым кодексом Российской Федерации, 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», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности краевого государственного казенного учреждения «Централизованная бухгалтерия по ведению учета в сфере социальной поддержки и социального обслуживания граждан» (Приложение № 1 к приказу).
2. Контроль за выполнением приказа оставляю за собой.

Директор Л. П. Жиглова

Приложение № 1 к приказу КГКУ «ЦБ»
от «02» 09.2020 №815-716

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ краевого государственного казенного учреждения «Централизованная бухгалтерия по ведению учета в сфере социальной поддержки и социального обслуживания граждан» (сокращенное наименование – КГКУ «ЦБ»)

г. Красноярск, 2020

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Политика информационной безопасности (далее – Политика ИБ) КГКУ «ЦБ» определяет цели и задачи системы обеспечения информационной безопасности (далее – ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется КГКУ «ЦБ» в своей деятельности.

1.2. Настоящая Политика ИБ распространяется на все территориальные отделения КГКУ «ЦБ» и обязательна для исполнения всеми его сотрудниками и должностными лицами.

1.3. Политика ИБ разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», другими действующими нормативными правовыми актами Российской Федерации.

1. ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ ОПРЕДЕЛЕНИЙ, ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ.

2.1. Для целей настоящей Политики ИБ используются следующие основные понятия:

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор информационной безопасности (АИБ) – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Доступ к информации – возможность получения информации и ее использования.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность (ИБ) – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

Информационная система (ИС) – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений КГКУ «ЦБ».

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные ресурсы (ИР) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

Конфиденциальная информация (КИ) – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений КГКУ «ЦБ» или иного вида ущерба.

Локальная вычислительная сеть (ЛВС) – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью КГКУ «ЦБ» и внешними сетями (сетью Интернет).

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Политика информационной безопасности (ПИБ) – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в КГКУ «ЦБ» для обеспечения его информационной безопасности.

Пользователь локальной вычислительной сети – сотрудник организации (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Программное обеспечение (ПО) – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Ответственный за техническое обеспечение – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети КГКУ «ЦБ».

Угрозы информации – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

АРМ – Автоматизированное рабочее место.
МЭ – Межсетевой экран.
ЛВС — Локальная вычислительная сеть.
НСД – Несанкционированный доступ.
ОС – Операционная система.
ПБ – Политики безопасности.
ПДн – Персональные данные.
СЗИ – Средство защиты информации.
СУИБ — Система управления информационной безопасностью.
ЭВМ – Электронная – вычислительная машина, персональный компьютер.

3. ЦЕЛИ НАСТОЯЩЕЙ ПОЛИТИКИ

3.1. Политика ИБ направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов

3.2. Основными целями Политики ИБ являются защита информации КГКУ «ЦБ» от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в «Положении о защите персональных работников краевого казенного учреждения «Централизованная бухгалтерия по ведения учета в сфера социальной поддержки и социального обслуживания граждан».

4. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Основными принципами обеспечения ИБ являются:

– постоянный и всесторонний анализ информационного пространства КГКУ «ЦБ» с целью выявления уязвимостей информационных активов;

– своевременное обнаружение проблем, потенциально способных повлиять на ИБ КГКУ «ЦБ», корректировка моделей угроз и нарушителя;

– разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей КГКУ «ЦБ», а также повышать трудоемкость технологических процессов обработки информации;

– контроль эффективности принимаемых защитных мер;

– персонификация и адекватное разделение ролей и ответственности между сотрудниками КГКУ «ЦБ», исходя из принципа персональной и единоличной ответственности за совершаемые операции.

5. ОТВЕТСТВЕННОСТЬ ЗА РЕАЛИЗАЦИЮ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

5.2. Ответственность за реализацию политики возлагается:

– в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на АИБ;

– в части, касающейся доведения правил политики до сотрудников КГКУ «ЦБ», а также иных лиц – на АИБ;

– в части, касающейся исполнения правил политики, – на каждого сотрудника КГКУ «ЦБ», согласно их должностным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

6. ЗАЩИЩАЕМЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ КГКУ «ЦБ»

6.1. Защищаемые информационные ресурсы: базы данных, содержащие персональные данные субъектов.

7. ПРЕДОСТАВЛЕНИЕ ДОСТУПА К ИНФОРМАЦИОННОМУ РЕСУРСУ

7.1. Допуск сотрудников КГКУ «ЦБ» к информации, содержащей персональные данные, осуществляется в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими должностных обязанностей.

7.2. Допуск сотрудника КГКУ «ЦБ» к информационным ресурсам ИСПДн оформляется заявкой, которая предоставляется начальником соответствующего отдела. В заявке указывается, к каким ресурсам и с какими правами (полномочиями) допустить конкретного сотрудника.

7.3. Заявка передается в отдел автоматизации бухгалтерского учета и развития информационной технологий.

Отдел автоматизации бухгалтерского учета и развития информационной технологий рассматривает представленную заявку и совершает необходимые операции по созданию учетной записи пользователя.

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания. Копии исполненных заявок хранятся у АИБ.

7.4. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника), учетная запись должна блокироваться.

7.5. АИБ проверяется соответствие требуемых прав доступа с реально необходимыми для выполнения должностных (функциональных) обязанностей данного работника.

7.6. Информационные ресурсы, формируемые в ИС подразделяются на:

– сетевые ресурсы с ограниченным доступом (базы данных и т.п.);

– ресурсы общего пользования (справочно-информационные системы, библиотеки, каталоги и т.п.);

– корпоративная электронная почта;

– сетевые принтеры;

– ресурсы пользователя (сетевые или локальные).

7.7. Решение о формировании новых информационных ресурсов и изменении существующих принимает начальник отдела, инициирующего это решение. В заявке на формирование обосновывается необходимость создания новых информационных ресурсов и указывается, в интересах каких групп пользователей они создаются.

7.8. Непосредственное формирование нового сетевого информационного ресурса осуществляется сотрудником отдела автоматизации бухгалтерского учета и развития информационных технологий. На исполненной заявке проставляется отметка о создании и местонахождении ресурса.

8. ПРАВИЛА ФОРМИРОВАНИЯ УЧЕТНЫХ ЗАПИСЕЙ

8.1. Учетные записи подразделяются на:

– пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов КГКУ «ЦБ»;

– системные – используемые для нужд операционной системы;

– служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

8.2. Каждому пользователю информационных активов КГКУ «ЦБ» назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, должно согласоваться с АИБ.

9. ПРЕДОТВРАЩЕНИЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ИЗВНЕ И УТЕЧЕК ПО ТЕХНИЧЕСКИМ КАНАЛАМ.

9.1. Для предотвращения угроз несанкционированного доступа извне и утечки информации по техническим каналам используются методы и оборудование в соответствии с Постановлением Совета Министров – Правительства Российской Федерации № 912-51 от 15.09.1993 «Об утверждении Положения о государственной

системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам».

9.2. В перечень мер входит:

- размещение серверов в защищенном дата центре;
- использование защищенных каналов связи;
- защита периметра локальной сети межсетевым экраном.

10.РЕАЛИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ

10.1. К использованию в КГКУ «ЦБ» допускаются только лицензионные и сертифицированные антивирусные средства. Изменение используемого антивирусного средства необходимо согласовать с АИБ. Установка средств антивирусного контроля на рабочих станциях и серверах ИС осуществляется АИБ.

10.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

11.ЛИКВИДАЦИЯ ПОСЛЕДСТВИЙ НАРУШЕНИЯ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11.1. АИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым информационным ресурсом ИС рекомендуется уведомить АИБ, и далее следовать их указаниям.

Действия АИБ и администратора информационной системы при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

– Инструкцией по обеспечению информационной безопасности;

– политикой информационной безопасности;

– регламентом администратора информационной безопасности.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

12.ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ

12.1. Ответственность за невыполнение ПИБ несет каждый сотрудник КГКУ «ЦБ» в рамках своих должностных обязанностей в соответствии с законодательством Российской Федерации.