УТВЕРЖДЕНА
приказом {Название Организации}
от «___» _____20__г. № ___

Инструкция пользователя государственной информационной системы «Бухгалтерия и кадры» {Название Организации}

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. С целью автоматизации процессов, в {Название организации} введена в действие ГИС «Бухгалтерия и кадры».

1.2. К работе с компонентами ГИС допущены системные администраторы, администратор информационной безопасности (далее - Администратор) и пользователи информационной системы (далее - Пользователи). В {Название организации} назначен ответственный за организацию обработки персональных данных (далее - Ответственный).

1.3. С целью защиты информации от несанкционированного нарушения ее конфиденциальности, целостности и доступности в ГИС организационными и техническими средствами реализована система защиты информации.

1.4. Несмотря на то, что многие действия по защите информации производятся прозрачно для Пользователя, он остается активным участником процесса по защите конфиденциальной информации и является вовлеченным в процессы обеспечения информационной безопасности в {Название организации}.

1.5. Пользователи ГИС не являются привилегированными пользователями информационной системы и получают доступ к ресурсам информационной системы в соответствии с Положением о разграничении доступа в ГИС «Бухгалтерия и кадры» (Приложение № 2 к Политике информационной безопасности). Каждому Пользователю предоставляется минимально необходимый для выполнения своих служебных обязанностей доступ к ресурсам ГИС.

1.6. Пользователи ГИС при работе с техническими средствами и информационными технологиями, являющимися частью ГИС должны соблюдать положения настоящей Инструкции.

1.7. Настоящая инструкция разработана с учетом положений следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;

- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

2. ОБЩИЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ГИС

2.1. Пользователь в ГИС выполняет только те действия, которые необходимы для выполнения его служебных обязанностей. Любые посторонние действия в ГИС запрещены.

2.2. Пользователь подписывает соглашение о неразглашении конфиденциальной информации перед началом выполнения служебных обязанностей, связанных с доступом к такой информации.

2.3. Пользователь незамедлительно оповещает Администратора о любой подозрительной активности в ГИС.

2.4. Пользователю запрещено использовать личные технические средства (ноутбуки, смартфоны, планшеты, фотокамеры, флеш-носители, съемные жесткие диски и пр.) для несанкционированного копирования, фотографирования, распространения и передачи защищаемой информации.

2.5. Пользователь принимает участие в инструктажах по информационной безопасности, проводимым Администратором и Ответственным. При получении дополнительных материалов от Администратора и Ответственного во время инструктажей, Пользователь самостоятельно изучает их с целью повышения своей осведомленности в вопросах информационной безопасности и защиты персональных данных.

2.6. Пользователь визуально контролирует целостность технических средств на своем рабочем месте (отсутствие попыток физического вскрытия системного блока и пр.). При подозрении на нарушение целостности технических средств ГИС, Пользователь сообщает об этом Администратору. Пользователю запрещен самостоятельный ремонт технических средств ГИС, а также привлечение посторонних лиц для такого ремонта.

2.7. В случае объективной необходимости, Пользователь участвует в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности.

2.8. В целях блокирования возможности несанкционированного ознакомления с защищаемой информацией на экране монитора, Пользователь должен блокировать сеанс работы в ГИС при покидании рабочего места более чем на 2 минуты. Блокировка сеанса работы в ГИС производится нажатием клавиш Win+L.

2.9. Пользователю запрещены любые действия в ГИС до прохождения процедуры идентификации и аутентификации в системе (до ввода логина и пароля).

2.10. Пользователю запрещено изменение источника загрузки своего автоматизированного рабочего места (далее - АРМ) и загрузка АРМ с внешних носителей.

2.11. Антивирусная защита в ГИС реализована прозрачно для пользователя, установка антивирусных программ, обновление антивирусных баз, запуск антивирусных проверок, сбор информации о найденных вирусах производится Администратором централизованно. Пользователю запрещено изменять настройки антивирусного программного обеспечения или отключать его (даже на короткое время). Пользователь должен оповещать Администратора о локальных сообщениях антивирусного программного обеспечения на его АРМ. Пользователь должен оповещать Администратора о любых аномалиях в работе АРМ. К таким аномалиям могут относиться:

- {перечислить}

2.12. Пользователю запрещается самостоятельная установка любого программного обеспечения, даже необходимого для выполнения своих служебных обязанностей. Установка разрешенного в ГИС программного обеспечения осуществляется Администратором и системными администраторами ГИС. Также к установке и настройке программного обеспечения в ГИС, при условии соблюдения мер по защите информации, допускаются сотрудники сторонних организаций.

2.13. Пользователь должен пресекать попытки посторонних лиц (или лиц, не имеющих соответствующих полномочий) тем или иным образом получить доступ к его учетным данным, конфиденциальной информации в ГИС, ключевой информации криптосредства и к любой другой защищаемой информации. Пользователь незамедлительно сообщает Администратору о подобных попытках (как удачных, так и неудачных).

2.14. Администратор отключает возможность использования на АРМ технологий мобильного кода (JavaScript, Adobe Flash, макросы в Microsoft Office и др.). Пользователю запрещено использовать технологии мобильного кода в обход принятых в {Название организации} политик информационной безопасности.

2.15. Пользователь в меру своих сил и возможностей содействует проведению служебных расследований, инициированных в связи с инцидентами информационной безопасности.

2.16. В {Название организации} действует политика управления информационными потоками и фильтрации сетевого трафика. Пользователь работает только с теми сетевыми ресурсами (сетевые папки, веб сайты и пр.), которые разрешены и, работа с которыми необходима Пользователю для выполнения

своих служебных обязанностей. Белый список внешних сетевых ресурсов приведен в приложении к Политике информационной безопасности. Пользователь имеет право сделать запрос Администратору на разрешение работы с заблокированными сетевыми ресурсами, обосновав необходимость внесения нового ресурса в белый список. Пользователю запрещено получать доступ к запрещенным внешним ресурсам в обход политик безопасности.

2.17. Пользователь осуществляет обработку защищаемой информации в ГИС в соответствии с технологическими процессами обработки информации, описанными в Политике информационной безопасности.

2.18. Пользователь принимает меры по противодействию несанкционированному просмотру защищаемой информации с экрана монитора посторонними лицами. К таким мерам относятся:

- сворачивание окна, в котором отображена защищаемая информация или блокирование сеанса Пользователя при нахождении посторонних лиц вблизи рабочего места Пользователя с фронтальной стороны монитора;
- ориентация монитора задней частью к дверным проемам и окнам;
- в случае вынужденной ориентации монитора фронтальной частью к окну, Пользователь во время работы с защищаемой информацией закрывает шторы, жалюзи или рольставни.

2.19. Пользователь должен знать и соблюдать положения настоящей Инструкции, а также других внутренних нормативных документов {Название организации}. При возникновении у Пользователя вопросов по защите информации и защите персональных данных в {Название организации}, он обращается к Администратору и Ответственному. Новые Пользователи ГИС перед началом выполнения своих служебных обязанностей изучают положения настоящей Инструкции.

2.20. При работе с криптографическими средствами защиты информации (СКЗИ) Пользователь выполняет предписание Инструкции по обеспечению безопасности эксплуатации СКЗИ.

3. ПРАВИЛА УПРАВЛЕНИЯ ИДЕНТИФИКАТОРАМИ, УЧЕТНЫМИ ЗАПИСЯМИ И ПАРОЛЯМИ

3.1. В {Название организации} с целью обеспечения информационной безопасности внедрены политики управления идентификаторами, учетными записями и паролями.

3.2. Внутренними руководящими документами, определяющими политики управления идентификаторами, учетными записями и паролями являются:

- политика информационной безопасности;
- порядок разграничения доступа к ресурсам ГИС;
- инструкция администратора информационной безопасности;
- инструкция пользователя ГИС.

3.3. Пользователь перед началом работы в ГИС получает учетные данные (персональный идентификатор, логин, временный пароль) у Администратора. Администратор выдает учетные данные Пользователю на основании заявки, заполненной по форме, приведенной в приложении № 1 к политике информационной безопасности.

3.4. При первом входе в систему Пользователь изменяет первичный временный пароль, назначенный ему Администратором. Временной промежуток между выдачей временного пароля и первым входом Пользователя в информационную систему не должен составлять более одного часа. Пароли должны соответствовать следующим требованиям:

- минимальная длина пароля составляет 8 символов, пароль должен содержать буквы английского алфавита верхнего и нижнего регистров, как минимум одну цифру и один спецсимвол;
- новый пароль должен отличаться минимум на два символа от предыдущего;
- запрещается использование пользователями пяти последних использованных паролей при создании новых паролей.

3.5. Максимальное время действия пароля - 90 дней. По истечении срока действия пароля, Пользователь должен придумать новый пароль, удовлетворяющий требованиям к паролям (п. 3.4 настоящей инструкции).

3.6. При восьми неудачных попытках входа, учетная запись Пользователя блокируется. Для разблокировки учетной записи Пользователю необходимо обратиться к Администратору.

3.7. Пользователю запрещено записывать и хранить пароли в местах, доступных для просмотра посторонним лицам (на отдельных листах бумаги, в не запираемой тумбе, под клавиатурой, на мониторе и т. п.).

3.8. Пользователь должен удостовериться, что при вводе пароля никто не наблюдает за процессом ввода пароля.

3.9. Пользователю запрещено разглашать другим пользователям свой пароль, в том числе Администратору.

3.10. Пользователю запрещено вводить свои учетные данные для предоставления возможности временной работы в ГИС другим Пользователями или посторонним лицам, поскольку все выполненные этими лицами действия в ГИС будут считаться действиями, выполненными Пользователем. Ответственность за неправомерные действия таких посторонних лиц несет Пользователь.

3.11. Пользователю запрещено оставлять без присмотра персональный идентификатор (электронный ключ).

3.12. При подозрении на компрометацию пароля или иной идентификационной информации, Пользователь должен незамедлительно сообщить об этом Администратору.

4. ПРОТИВОДЕЙСТВИЕ МЕТОДАМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ПРАВИЛА РАБОТЫ С ЭЛЕКТРОННОЙ ПОЧТОЙ

4.1. Применение злоумышленником методов социальной инженерии является самым эффективным и разрушительным способом нарушения информационной безопасности на любом предприятии в обход всех технических мер по защите информации. Методы социальной инженерии направлены на использование человеческого фактора (человеческих слабостей и недостатков) с целью получения от Пользователя защищаемой информации или его учетных данных в ГИС (логин и пароль). Злоумышленники

- социальные инженеры для достижения своих целей могут эксплуатировать следующие особенности того или иного Пользователя:

- лень;
- спешка (паника);
- безразличие;
- профессиональный интерес;
- желание;
- жадность;
- сострадание;
- доверчивость;
- страх.

4.2. Основным способом реализации методов социальной инженерии является обман Пользователя. Поскольку социальная инженерия нацелена на слабости человека, а не на технические недоработки или уязвимости информационной системы, наиболее эффективным методом противодействия социальной инженерии является повышение осведомленности Пользователей о методах социальной инженерии.

4.3. Взаимодействие социального инженера с Пользователем бывает трех типов: контактное (личное), телефонное и взаимодействие через электронные каналы связи. Наиболее распространено взаимодействие через электронные каналы связи, в особенности по электронной почте.

4.4. При личном и телефонном общении Пользователь должен убедиться, что разговаривает именно с тем человеком, за которого себя выдает собеседник. При личном или телефонном взаимодействии социальный инженер обычно использует следующие тактики:

- представившись сотрудником технической поддержки какого-либо сервиса или службы, социальный инженер сообщает Пользователю о какой-либо поломке или нарушении в функционировании того или иного необходимого в работе сервиса, вызывая тем самым панику и заставляя Пользователя сообщить свои учетные данные;
- представившись руководителем высокого ранга, социальный инженер изображает гнев и недовольство действием или бездействием Пользователя, вынуждая сообщить учетные данные или иную конфиденциальную информацию;
- представившись сотрудником организации, деятельность которой так или иначе может быть интересна Пользователю вынуждает сообщить учетную или иную конфиденциальную информацию;
- иные подобные тактики.

4.5. При взаимодействии через электронную почту, социальный инженер преследует одну из двух основных целей:

- заражение АРМ Пользователя вредоносным программным обеспечением через запуск приложенного к письму файла или переходом по вредоносной ссылке;
- переход Пользователя по поддельной ссылке, по которой находится точная копия формы авторизации легального сервиса и ввод в эту форму идентификационной информации (как правило, при первом вводе логина и пароля поддельная форма сообщает о неправильном вводе пароля и перенаправляет на настоящую форму авторизации сервиса).

4.6. Наиболее распространенные примеры применения методов социальной инженерии с использованием каналов электронной почты:

- письмо от налоговой инспекции с предложением установить из вложенного файла новые формы для сдачи налоговых деклараций;
- письмо из банка о просроченном платеже по кредиту, подробности во вложенном файле;
- письмо из суда о возбуждении административного/уголовного дела, подробности во вложении;
- письмо от провайдера об одностороннем изменении тарифного плана, подробности во вложении;
- письмо от банка (или любого другого учреждения) о блокировке учетной записи на сайте или личного кабинета, необходимо пройти по ссылке, ввести учетные данные и вручную разблокировать личный кабинет или учетную запись;
- письмо от сервиса электронной почты (gmail.com, mail.ru, yandex.ru и т. п.) о грядущей блокировке почтового ящика, об исчерпании свободного места и т. д., необходимо пройти по ссылке, ввести учетные данные и выполнить некоторые действия.

4.7. При работе с электронной почтой в контексте противодействия методам социальной инженерии Пользователь руководствуется следующей информацией:

- совпадение адреса отправителя электронного письма с доверенным адресом не является гарантией подлинности самого письма, поскольку поле «от кого» может быть подделано злоумышленником;
- любые письма с вложениями являются подозрительными;
- любые письма, в которых отсутствует альтернативная контактная информация отправителя (ФИО, должность, мобильный, рабочий телефон, почтовый адрес) являются подозрительными;
- при получении неожидаемого электронного письма с вложением или ссылкой от якобы доверенного отправителя, необходимо по альтернативным каналам связи (лично, по телефону, через мессенджер) уточнить факт отправки такого письма;
- государственные и иные организации (банки, операторы связи и т. д.) не уведомляют своих клиентов о каких-либо проблемах, исках, блокировках по электронной почте, это делается официальным письмом на бумажном носителе, через СМС (например, в случае подключенного он-лайн банкинга) или по телефону;
- необходимо тщательно проверять корректность ссылок, по которым просят пройти в письме, чаще всего злоумышленники используют похожие, но другие доменные имена, чтобы ввести Пользователя в заблуждение, например, заменяя букву “b” на букву “d” или цифру “1” на букву “l” и наоборот.

4.8. Атаки социальных инженеров могут быть веерными (нацеленными на как можно большее число жертв), так и целенаправленными (нацеленными на конкретную организацию или на конкретного человека). В случае целенаправленных атак, социальный инженер изучает информацию о потенциальной жертве и об организации из открытых источников (сайт компании, сайты партнеров и контрагентов, электронные биржи труда, социальные сети, новостные ленты и прочие ресурсы). В случае, если о Пользователе публикуется информация в открытых источниках или он сам публикует информацию о своем месте работы, роде деятельности,

должностных обязанностях, Пользователь должен быть готов к применению этой информации социальным инженером против него.

4.9. В случае подозрения Пользователя на применение против него методов социальной инженерии, Пользователь незамедлительно сообщает о данном факте Администратору.

5. РАБОТА СО СЪЕМНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

5.1. Пользователю разрешается использовать только учтенные съемные носители информации в ГИС (флешки, съемные жесткие диски, карты памяти и пр.).

5.2. При необходимости использования для исполнения служебных обязанностей съемных носителей информации Пользователь в письменной форме делает запрос Администратору на выдачу учтенного съемного носителя информации. Пользователь расписывается за получение и сдачу учтенного съемного носителя информации в Журнале учета носителей информации.

5.3. При необходимости выноса съемного носителя из помещения, Пользователь обеспечивает защиту съемного носителя от утери, кражи или компрометации защищаемой информации на этом носителе.

5.4. В случае утери, кражи или компрометации учтенного носителя, Пользователь оперативно сообщает об этом Администратору.

5.5. Пользователь несет ответственность за сохранность выданных ему съемных носителей информации и за конфиденциальность защищаемой информации, записанной на него.