В случае производственной необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имён (учётных записей).

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

В общем случае запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учётной записи должно сопровождаться отметкой в журнале учёта машинного времени, которая должна однозначно идентифицировать текущего владельца учётной записи в каждый момент времени. Одновременное использование одной общей пользовательской учётной записи разными пользователями запрещено.

Регистрируемые учётные записи подразделяются на:

- Пользовательские – предназначенные для аутентификации пользователей ИР Учреждения;
- Системные – используемые для нужд операционной системы;
- Служебные – предназначенные для функционирования отдельных процессов или приложений.

Системные учётные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные учётные записи используются только для запуска и работы сервисов или приложений.

Использование системных или служебных учётных записей для регистрации пользователей в системе категорически запрещено.

Процедуры регистрации и блокирования учётных записей пользователей должны применяться с соблюдением следующих правил:

- использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершёнными ей действиями;
- использование групповых ID разрешать только в случае, если это необходимо для выполнения задачи;
- предоставление и блокирование прав должны быть санкционированы и документированы;
- предоставление прав доступа к ИР, только после согласования с владельцем данного ИР;
- регистрация и блокирование учётных записей допускается с отдельного разрешения руководства Учреждения;
- уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;
- согласование изменения прав доступа с отделом ИС СМТ;
- документальная фиксация назначенных пользователю прав доступа;
- ознакомление пользователей под подпись с письменными документами, в которых регламентируются их права доступа;
- предоставление доступа с момента завершения процедуры регистрации;
- обеспечение создания и поддержания формального списка всех пользователей, зарегистрированных для работы с ИР или сервисом;
- немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из Учреждения;
- аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;

- обеспечение того, чтобы лишние ID пользователей не были доступны другим пользователям;
- обеспечить возможность предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путем суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

1. Управление привилегиями

Доступ сотрудника к информационным ресурсам Учреждения должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный сотрудник, и владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами.

Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий. Должны быть рассмотрены следующие этапы:

- должны быть идентифицированы привилегии доступа, связанные с каждым системным продуктом, например, с операционной системой, системой управления базой данных и каждым приложением, а также пользователи, которым они должны быть предоставлены;
- привилегии должны предоставляться пользователям на основании «производственной необходимости» и только на период времени, необходимый для достижения поставленных целей, например, привилегии, минимально необходимые для выполнения их функциональных обязанностей, только тогда, когда эти привилегии необходимы;
- должен быть обеспечен процесс санкционирования всех предоставленных привилегий и создание отчетов по ним, привилегии нельзя предоставлять до завершения процесса их регистрации;
- уникальные привилегии должны присваиваться на другой ID пользователя, не тот, который используется при обычной работе пользователя.

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Учреждения осуществляется в процессе аудита ИБ в соответствии с Правилами аудита ИБ и установленными процедурами.

2. Управление паролями

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

- все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;
- при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;
- временные пароли должны назначаться пользователю только после его идентификации;
- необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;
- временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;
- пользователь должен подтвердить получение пароля;
- пароли должны храниться в электронном виде только в защищенной форме;
- назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;

- необходимо установить требования к длине пароля, набору символов и числу попыток ввода;
- необходимо изменять пароля пользователя не реже одного раза в 90 дней.

При необходимости можно рассмотреть возможность использования других технологий идентификации и аутентификации пользователей, в частности, биометрических технологий, проверки подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

3. Контроль прав доступа

Чтобы обеспечить эффективный контроль доступа необходимо ввести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

- права доступа пользователей должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИС;
- права доступа пользователей должны проверяться и переназначаться при изменении их должностных обязанностей в Учреждении, а также при переходе с одной работы на другую в пределах Учреждения;
- проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться чаще (не реже одного раза в 3 месяца);
- необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;
- изменение привилегированных учетных записей должно протоколироваться.

Контроль над выполнением процедур управления доступом пользователей должен включать:

- контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации;
- проверку подлинности пользователей перед сменой паролей;
- немедленное блокирование прав доступа при увольнении;
- блокирование учётных записей, неактивных более 45 дней;
- включение учётных записей, используемых поставщиками для удалённой поддержки, только на время выполнения работ;
- отслеживание удалённых учётных записей, используемых поставщиками, во время работ;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение не менее трёх лет;
- ознакомление с правилами и процедурами аутентификации всех пользователей, имеющих доступ к сведениям ограниченного распространения;
- использование механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;
- разрешение запросов и прямого доступа к базам данных только для администраторов баз данных;
- блокирование учётной записи на период равный 30 минутам или до разблокировки учётной записи администратором;
- блокирование учетных записей пользователей при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации.

4. Использование паролей

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых сотруднику Учреждения предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) сотрудником информации.

Не допускается использование различными пользователями одних и тех же учётных данных.

Первоначальное значение пароля учетной записи пользователя устанавливает Администратор безопасности.
Личные пароли устанавливаются первый раз сотрудниками отдела ИС СМТ. После первого входа в систему и в дальнейшем пароли выбираются пользователями автоматизированной системы самостоятельно с учетом установленных требований
Сотруднику запрещается:

- сообщать свой пароль кому-либо;
- указывать пароль в сообщениях электронной почты;
- хранить пароли, записанные на бумаге, в легко доступном месте;
- использовать тот же самый пароль, что и для других систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.);
- использовать один и тот же пароль для доступа к различным корпоративным ИС.

Вход пользователя в систему не должен выполняться автоматически.
Учреждение оставляет за собой право:

- осуществлять периодическую проверку стойкости паролей пользователей, используемых сотрудниками для доступа к ИС;
- принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей политики.

5. Пользовательское оборудование, оставляемое без присмотра

Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра. Все пользователи должны быть осведомлены о требованиях ИБ и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

6. Политика чистого стола

Сотрудники Учреждения обязаны:

- сохранять известные им пароли в тайне;
- закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищённый паролем хранитель экрана;
- по завершении сеанса выходить из системы у универсальных ЭВМ, серверов и офисных ПК.

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утверждён.
Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.
Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра.
Вход пользователя в систему не должен выполняться автоматически.

Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.
В конце рабочего дня сотрудник должен привести в порядок письменный стол и убрать все офисные документы в запираемый шкаф или сейф.
Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги.

По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

7. Мобильное компьютерное оборудование

При использовании мобильных средств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Учреждению. Необходимо принять официальную политику, учитывающую риск, связанный с использованием мобильных компьютеров, и в частности с работой в незащищённой среде.

Шаблон 4

Политика допустимого использования информационных ресурсов

Общие обязанности пользователя:

- при работе с ПО руководствоваться нормативной документацией (руководством пользователя);
- обращаться в службу поддержки пользователей или к специалистам, назначенными ответственными за системное администрирование и информационную безопасность, по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), а также за необходимой методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;
- знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;
- минимизировать вывод на печать обрабатываемой информации.

Пользователю запрещено производить несанкционированное распространение справочной информации, которая становится доступна при подключении к корпоративной ИС Учреждения.

1. Использование ПО

На АРМ <название организации> допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения.

Запрещено незаконное хранение на жестких дисках АРМ <название организации> информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

Решение о приобретении и установке программного обеспечения, необходимого для реализации медицинских, финансовых, административно-хозяйственных и других задач принимает <должность ответственного> по представлении начальника <название ответственного отдела>.

Документы, подтверждающие покупку программного обеспечения, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся в <название ответственного отдела>.

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ <название организации>. Указанные работы, а так же работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только сотрудниками <название ответственного отдела>.

Сведения о вновь приобретённом программном обеспечении должны быть внесены в перечень разрешённого программного обеспечения.
Перечень разрешенного программного обеспечения в ГИС «Бухгалтерия и кадры» определен в Приложении № 4 к настоящей Политике.

2. Использование АРМ и ИС

К работе в ИС Учреждения допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.
Каждому сотруднику Учреждения, которому необходим доступ к ИР в рамках его должностных обязанностей, выдаются под роспись необходимые средства автоматизации. Ответственность по установке и поддержке всех компьютерных систем, функционирующих в Учреждении, возложена на отдел ИС СМТ.
Каждый сотрудник Учреждения, обеспеченный АРМ, получает персональное сетевое имя, пароль, адрес электронной почты и личный каталог в сети, который предназначен для хранения рабочих файлов.
Работа в ИС сотрудникам разрешена только на закреплённых за ними АРМ, в определённое время и только с разрешенным программным обеспечением и сетевыми ресурсами.
Все АРМ, установленные в Учреждении, имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией, определённый в стандарте рабочих мест Учреждения. Изменение установленной конфигурации возможно после внесения соответствующих поправок в стандарт рабочих мест или по служебной записке, согласованной с отделом ИС СМТ. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется отделом ИС СМТ.
Самостоятельная установка программного обеспечения на АРМ запрещена. Установка и удаление любого программного обеспечения производится только сотрудниками отдела ИС СМТ.
В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в отдел ИС СМТ.
Сотрудники отдела ИС СМТ имеют право осуществлять контроль над установленным на компьютере программным обеспечением, и принимать меры по ограничению возможностей несанкционированной установки программ.
Передача документов внутри Учреждения производится только посредством общих папок, а также средствами электронной почты.
При работе в ИС Учреждения сотрудник обязан:

- знать и выполнять требования внутренних организационно-распорядительных документов Учреждения;
- использовать ИС и АРМ Учреждения исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИС СМТ о любых фактах нарушения требований ИБ;
- ставить в известность отдел ИС СМТ о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;
- незамедлительно выполнять предписания отдела ИС СМТ Учреждения.
- Предоставлять АРМ сотрудникам отдела ИС СМТ для контроля;
- При необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;
- В случае необходимости продолжения работы по окончании рабочего дня проинформировать об этом отдел ИС СМТ.

При использовании ИС Учреждения запрещено:

- использовать АРМ и ИС в личных целях;

- отключать средства управления и средства защиты, установленные на рабочей станции;
- передавать:
- конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с отделом ИС СМТ;
- информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;
- угрожающую, клеветническую, непристойную информацию;
- самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС Учреждения;
- предоставлять сотрудникам Учреждения (за исключением администраторов ИС и ИБ) и третьим лицам доступ к своему АРМ;
- запускать на АРМ ПО, не входящее в Реестр разрешенного к использованию ПО;
- защищать информацию, способами, не согласованными с отделом ИС СМТ заранее;
- самостоятельно подключать рабочую станцию и прочие технические средства к корпоративной ИС Учреждения;
- осуществлять поиск средств и путей повреждения, уничтожения технических средств и ресурсов ИС или осуществлять попытки несанкционированного доступа к ним;
- использовать для выполнения служебных обязанностей локальные (не доменные) учетные записи АРМ.

Информация о посещаемых ресурсах ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Учреждения.
Все электронные сообщения и документы в электронном виде, передаваемые посредством ИС Учреждения подлежат обязательной проверке на отсутствие вредоносного ПО.

3. Использование ресурсов локальной сети

Для выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Учреждения, базы данных, электронная почта.
Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы. Доступ сотрудников к ресурсам сети осуществляется согласно матрицы доступа. Временное расширение прав доступа осуществляется отделом ИС СМТ Учреждения в соответствии с Порядком предоставления (изменения) полномочий пользователя.

4. Обработка конфиденциальной информации

При обработке конфиденциальной информации сотрудники обязаны:

- знать и выполнять требования Инструкции по работе с конфиденциальной информацией;
- при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети Учреждения применять средства защиты от неавторизованного доступа;
- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;
- не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;
- обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;

- не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;
- не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;
- не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD – диски, Flash – устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

5. Использование электронной почты

Электронная почта используется для обмена в рамках ИС Учреждения и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде.

Для обеспечения функционирования электронной почты допускается применение ПО, входящего в реестр разрешённого к использованию ПО.

При работе с корпоративной электронной почтой Учреждения пользователь должен учитывать:

- электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;
- электронная почта не является средством передачи информации, гарантирующим конфиденциальность передаваемой информации (передачу конфиденциальной информации вне локальной сети Учреждения необходимо осуществлять только в зашифрованном виде);
- электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

Организацией и обеспечением порядка работы электронной почты в Учреждении занимается отдел ИС СМТ.

Каждый сотрудник Учреждения получает почтовый адрес вида name@er76.ru в домене Учреждения. Адрес электронной почты выдаётся сотрудником отдела ИС СМТ при начальной регистрации пользователя в домене Учреждения.

Корпоративная электронная почта Учреждения предназначена исключительно для использования в служебных целях.

Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Учреждению. Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты принадлежат Учреждению и являются неотъемлемой частью его производственного процесса.

Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах Учреждения либо удалены уполномоченными сотрудниками Учреждения.

Пользователям корпоративной электронной почты Учреждения запрещено вести частную переписку с использованием средств корпоративной электронной почты Учреждения. К частной переписке относится переписка, не связанная с исполнением сотрудником своих должностных обязанностей.

Использование корпоративной электронной почты Учреждения для частной переписки сотрудником, надлежащим образом, ознакомленным с данной Политикой, является нарушением трудовой дисциплины Учреждения. Подписываясь в ознакомлении с настоящей Политикой, сотрудник даёт согласие на ознакомление и иное использование в интересах Учреждения его переписки, осуществляемой с использованием корпоративной электронной почты, и соглашается с тем, что любое использование его переписки, осуществляемой с использованием корпоративной электронной почты, не может рассматриваться как нарушение тайны связи.

Каждый сотрудник Учреждения имеет право на просмотр либо иное использование в интересах Учреждения сообщений корпоративной электронной почты, которые направлены или получены им, соответственно, с его или на его корпоративный электронный адрес.
Использование сообщений корпоративной электронной почты осуществляется уполномоченными сотрудниками Учреждения в соответствии с их функциями, определёнными в данной Политике и в иных локальных нормативных актах Учреждения. Просмотр и иное использование сообщений электронной почты в интересах Учреждения осуществляется сотрудниками Учреждения в целях обеспечения защиты конфиденциальных сведений, обеспечения нормальной работоспособности системы электронной почты, в рамках обслуживания сервисов электронной почты, при выполнении ручной пересылки сообщений, приходящих на корпоративные электронные адреса Учреждения сотрудникам или группам сотрудников, а также по мотивированным запросам прямых или непосредственных руководителей любых сотрудников, чью почту необходимо использовать в интересах Учреждения.
Использование сообщений корпоративной электронной почты в интересах Учреждения, в том числе ознакомление с содержанием сообщений, осуществляется в соответствии с правами доступа к информации, установленными внутренними Положениями о конфиденциальной информации и иными правовыми актами, регламентирующими порядок обращения с информацией ограниченного доступа.
Исходящие электронные сообщения сотрудников Учреждения должны содержать следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (вложенные файлы);
- подпись отправителя;
- предупреждение о служебном характере сообщения и его конфиденциальности.

6. Работа в сети

Доступ к сети Интернет предоставляется сотрудникам Учреждения в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.
Для доступа сотрудников Учреждения к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.
При использовании сети Интернет необходимо:

- соблюдать требования настоящей Политики;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИС СМТ о любых фактах нарушения требований настоящей Политики.

При использовании сети Интернет запрещено:

- использовать предоставленный Учреждением доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Учреждения;
- Публиковать, загружать и распространять материалы содержащие:
  - Конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с отделом ИС СМТ;

- угрожающую, клеветническую, непристойную информацию;
- вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;
- фальсифицировать свой IP- адрес, а также прочую служебную информацию.

Учреждение оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Блокирование и ограничение доступа пользователей к Интернет-ресурсам осуществляется на основе Регламента применения категорий Интернет-ресурсов.

Информация о посещаемых сотрудниками Учреждения Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Учреждения для контроля.

Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

Шаблон 5

Политика использование мобильных устройств

Под использованием мобильных устройств (например, ноутбуков, планшетов и мобильных телефонов) и носителей информации в ИС Учреждения понимается их подключение к инфраструктуре ИС с целью обработки, приёма/передачи информации между ИС и мобильными устройствами, а также носителями информации.

На предоставленных Учреждением мобильных устройствах допускается использование ПО, входящего в Реестр разрешённого к использованию ПО.

К предоставленным Учреждением мобильным устройствам и носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ. Целесообразность дополнительных мер обеспечения ИБ определяется отделом ИС СМТ.

При использовании предоставленных Учреждением мобильных устройств и носителей информации, сотрудник обязан:

- соблюдать требования настоящей Политики;
- использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИС СМТ о любых фактах нарушения требований настоящей Политики;
- эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;
- обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;
- извещать отдел ИС СМТ о фактах утраты (кражи) мобильных устройств и носителей информации.

При использовании предоставленных сотрудника Учреждения мобильных устройств и носителей информации запрещено:

- использовать мобильные устройства и носители информации в личных целях;
- передавать мобильные устройства и носители информации другим лицам (за исключением администраторов ИС и ИБ);
- оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, приём\передача информации) инициированное сотрудником Учреждения между ИС и неучтёнными (личными) мобильным и устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговорённых с администраторами ИС заранее). Учреждение оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации;
Информация об использовании сотрудниками Учреждения мобильных устройств и носителей информации в ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также руководству Учреждения.
Информация, хранящаяся на предоставляемых Учреждением мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.
В случае увольнения, предоставленные ему мобильные устройства и носители информации изымаются.
Перечень разрешенного программного обеспечения в мобильных устройствах определен в Приложении № 5 к настоящей Политике.

Шаблон 6

Политика защиты от вредоносного ПО

Отдел ИС СМТ регулярно проверяет сетевые ресурсы Учреждения антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.
При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник Учреждения должен незамедлительно оповестить об этом отдел ИС СМТ. После чего администратор ИБ должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.
В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения заражения своего руководителя и отдел ИС СМТ, а также владельца файла и смежные подразделения, использующие эти файлы в работе.
- Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

Правила предупреждения вирусного заражения в ГИС «Бухгалтерия и кадры» определены в Инструкции пользователя по обеспечению безопасности информации при её обработке в ИС.

Шаблон 7

Политика управления установкой (инсталяцией) компонентов программного обеспечения

В ГИС «Бухгалтерия и кадры» разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Приложением № 7. Пользователям запрещена установка любого ПО в ГИС «Бухгалтерия и кадры».

Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ГИС программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей программ, утилит, драйверов. В такой служебной записке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.

Администратор ежемесячно с помощью инструмента XSpider 7.8.24 проводит проверку соответствия состава программного обеспечения в ГИС «Бухгалтерия и кадры» списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

На серверной части ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

На АРМ Пользователей ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

На АРМ Администратора ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

Шаблон 8

Политика обеспечения доверенной загрузки средств вычислительно техники

В {Название Организации} в качестве средства доверенной загрузки технических средств применяется {Название МДЗ}. {Убрать, если применяются компенсирующие меры}

Для работы с ресурсами ГИС «Бухгалтерия и кадры» выбираются такие технические средства, базовая система ввода-вывода которых (BIOS/UEFI) позволяет отключить возможность выбора источника загрузки в обход настроек BIOS/UEFI (вызов вариантов источников загрузки одной из функциональных клавиш).

Администратор контролирует работоспособность {Название МДЗ} в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяются компенсирующие меры}

В случае некорректной работы средства доверенной загрузки на техническом средстве, такое техническое средство изымается из ГИС на время проведения ремонта/замены средства доверенной загрузки. В случае необходимости продолжения работы на техническом средстве, применяются следующие компенсирующие меры {Убрать, если применяются компенсирующие меры}:

- опечатываются USB-порты, входы для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводы и сами технические средства;
- устанавливается пароль администратора на вход в BIOS/UEFI и отключается возможность вызова источника загрузки нажатием функциональной клавиши (F1-F12) при загрузке;
- устанавливается усиленный визуальный контроль за техническим средством.

В проектной документации на систему защиты информации в ГИС «Бухгалтерия и кадры» обосновано применение компенсирующих мер, нейтрализующих угрозы безопасности информации, связанные с недоверенной загрузкой технических средств ГИС. {Убрать, если применяется МДЗ}

В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется опечатывание USB-портов, входов для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводов и самих технических средств. Данная мера обеспечивает контроль доступа злоумышленника к интерфейсам ввода-вывода, позволяющим осуществить недоверенную загрузку. {Убрать, если применяется МДЗ}

В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется установка пароля администратора на вход в BIOS/UEFI и отключение возможности вызова источника загрузки во время загрузки технического средства. Данная мера позволяет блокировать на программном уровне изменение источника загрузки при срыве пломбы с интерфейса ввода-вывода. {Убрать, если применяется МДЗ}

В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется усиленный визуальный контроль за техническими средствами ГИС. Данная мера позволяет своевременно детектировать факты нарушения пломб технического средства, выявлять факты несанкционированного доступа и принимать меры реагирования. {Убрать, если применяется МДЗ}

Администратор контролирует выполнение компенсирующих мер в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяется МДЗ}

Шаблон 9

Политика использования криптографического контроля

Все, поступающие в Учреждение, СКЗИ должны быть учтены в соответствующем журнале поэкземплярного учёта СКЗИ.

В Учреждении должно осуществляться управление ключами для эффективного применения криптографических методов. Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации.

Все ключи должны быть защищены от изменения, утери и уничтожения. Кроме того, секретные и закрытые ключи должны быть защищены от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено.

Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям, таким как Интернет. Шифрование любой другой информации в ИС Учреждения должно осуществляться только после получения письменного разрешения на это.

1. Требований по обеспечению ИБ при использовании шифрования

Шифрование – это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.

СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Порядок применения СКЗИ определяется руководством Учреждения и должен включать:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой информацией;
- порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

Для шифрования конфиденциальной информации минимально допустимой длинной ключа является 128 бит.

При использовании шифрования в ИС Учреждения должны применяться только утверждённые стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

2. Электронные цифровые подписи

ЭЦП обеспечивают защиту аутентификации и целостности электронных документов.

ЭЦП могут применяться для любой формы документа, обрабатываемого электронным способом. ЭЦП должны быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой – для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

Криптографические ключи, используемые для цифровых подписей, должны отличаться от тех, которые используются для шифрования.

При использовании ЭЦП, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

3. Управление ключами

Управление криптографическими ключами важно для эффективного использования криптографических средств.

Любая компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации. Следует применять систему защиты для обеспечения использования в ИС Учреждения криптографических методов в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами должны использоваться для шифрования и для генерации цифровых подписей.

Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия. Криптографические методы могут также использоваться для этой цели. Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Сервер сертифицированного центра КУЦ должен хранить текущие открытые ключи для всех авторизованных на это сотрудников. Для безопасного взаимодействия с внешними пользователями ИС Учреждения необходимо использовать электронные сертификаты только из утверждённого списка сертифицированных центров.

Секретные ключи пользователей должны храниться так же, как и пароли. О любом подозрении на компрометацию секретного ключа пользователь должен немедленно доложить в отдел ИС СМТ.

Необходимо, чтобы система обеспечения безопасности использования ключей основывалась на согласовании способов, процедур и безопасных методов для:

- генерации ключей при использовании различных криптографических систем и приложений;
- генерации и получения сертификатов открытых ключей;
- рассылки ключей, предназначенных пользователям, включая инструкции по их активации при получении;
- хранения ключей (при этом необходимо наличие инструкции авторизованным пользователям для получения доступа к ключам);
- смены или обновления ключей, включая правила порядка и сроков смены ключей;
- порядка действий в отношении скомпрометированных ключей;
- аннулирования ключей, в том числе способы аннулирования или дезактивации ключей, если ключи были скомпрометированы или пользователь уволился из организации (в этом случае ключи необходимо архивировать);
- восстановление ключей, которые были утеряны или испорчены, для рассекречивания зашифрованной информации;
- архивирования и резервного копирования ключей;
- разрушения ключей;
- регистрация ключей и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации, для ключей необходимо определить даты начала и конца действия, чтобы их можно было использовать лишь в течении ограниченного периода времени, который зависит от обстоятельств использования криптографических средств, контроля и от степени риска раскрытия информации.

Может потребоваться наличие процедур обработки юридических запросов, касающихся доступа к криптографическим ключам, например, чтобы зашифрованная информация стала доступной в незашифрованном виде для доказательств в суде.

Необходимо обеспечивать защиту открытых ключей от угроз подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей. Сертификаты необходимо изготавливать таким способом, который однозначно связывал бы информацию, относящуюся к владельцу пары открытого/секретного ключей, с открытым ключом. Поэтом важно, чтобы процессу управления, в рамках которого формируются эти сертификаты, можно было доверять.

Соглашения с внешними поставщиками криптографических услуг (например, с удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

Шаблон 10

Политика резервного копирования

Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ГИС «Бухгалтерия и кадры» осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 10 к настоящей Политике.

Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ГИС «Бухгалтерия и кадры».

Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ГИС «Бухгалтерия и кадры».

Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

Нештатными ситуациями являются:

- разглашение информации ограниченного доступа сотрудниками {Название Организации}, имеющими к ней право доступа, в том числе:
  - разглашение информации лицам, не имеющим права доступа к защищаемой информации;
  - передача информации по незащищенным каналам связи;

- обработка информации на незащищенных технических средствах обработки информации;
- опубликование информации в открытой печати и других средствах массовой информации;
- передача носителя информации лицу, не имеющему права доступа к ней;
- утрата носителя с информацией.

- неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
  - несанкционированное изменение информации;
  - несанкционированное копирование информации;
- несанкционированный доступ к защищаемой информации:
  - несанкционированное подключение технических средств к средствам и системам ГИС «Бухгалтерия и кадры»;
  - использование закладочных устройств;
  - использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ГИС «Бухгалтерия и кадры»;
  - использование злоумышленником уязвимостей программного обеспечения ГИС;
  - использование злоумышленником программных закладок;
  - заражение ГИС злоумышленником программными вирусами;
  - хищение носителей информации;
  - нарушение функционирования технических средств обработки информации;
  - блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
- дефекты, сбои, отказы, аварии технических средств и систем ГИС;
- дефекты, сбои, отказы программного обеспечения ГИС;
- сбои, отказы и аварии систем обеспечения ГИС;
- природные явления, стихийные бедствия:
  - термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
  - механические факторы (повреждения зданий, землетрясения и т. д.);
  - электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.

Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 11 настоящей Политики.

С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

- корректное отключение технических средств ГИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ГИС а также меры по замене/ремонту вышедших из строя средств и систем;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:

- Пользователи корректно отключают и обесточивают свои рабочие места;
- системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;
- Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в ГИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;
- в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.

Шаблон 11

Политика контроля состава технических средств, программного обеспечения и средств защиты информации

Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ГИС «Бухгалтерия и кадры» фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

В случае добавления новых ТС, ПО и СрЗИ в состав ГИС «Бухгалтерия и кадры» или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.

Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ГИС «Бухгалтерия и кадры» является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.

В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе)

информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом руководителю {Название Организации}, который принимает решение об организации самостоятельной сертификации использующегося СрЗИ, либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

Шаблон 12

Политика дистанционной работы

1. Ответственность

Ответственность за установку, настройку и администрирование средств обработки информации на рабочем месте пользователя возлагается на службу информационных технологий или иную службу {Название Организации}.

Ответственность за соблюдение правил или политики организации рабочего места возлагается на всех работников фирмы и третьих лиц, использующих средства обработки информации.

Контроль выполнения политики организации рабочего места возлагается на службу информационной безопасности {Название Организации}.

Провести анализ

2. Назначение и область действия

Настоящая политика устанавливается для эффективной организации дистанционной работы пользователей в целях:

- Защиты сетевых сервисов;
- Предотвращения неавторизованного доступа к операционным системам;
- Обеспечение информационной безопасности при работе в дистанционном режиме.

Правила распространяются на всех работников фирмы и третьих лиц, участвующих в организации работы и работающих в дистанционном режиме, и являются обязательными для исполнения.

Все исключения из настоящих правил должны быть согласованы со службой информационной безопасности {Название Организации}..

3. Основные требования

Предоставление пользователю дистанционного доступа должно быть согласовано с руководителем подразделения данного сотрудника и владельцем информационных ресурсов, к которым предоставляется доступ. Управление дистанционным доступом осуществляется в соответствии с установленными процедурами.

Для контроля доступа пользователя в дистанционном режиме должны использоваться надежные методы аутентификации, включая:

- обратный вызов;
- аутентификацию узла по физическому адресу;
- решения для VPN;
- выделенные физические линии и т.д.

При использовании обратного вызова должна быть блокирована возможность переадресации

Доступ в дистанционном режиме обязательно организуется с использованием установленных средств шифрования траффика.
Дистанционный доступ к используемым диагностическим и конфигурационным портам оборудования должен регистрироваться. Возможность дистанционного доступа к неиспользуемым диагностическим или конфигурационным портам оборудования должна быть исключена.
Для сеансов дистанционного доступа должно быть установлено время бездействия, во время которого оборудование отключается, и сеанс работы прекращается.
Для критических приложений должно использоваться ограничение времени соединения дистанционного доступа.
Обязательными условиями предоставления дистанционного доступа к информационным ресурсам фирмы являются:

- Установка и своевременное обновление на компьютере пользователя средств антивирусной защиты.
- Установка и надлежащая настройка на компьютере пользователя применяемых в фирме или организации средств предотвращения атак.

Настройка локальных параметров безопасности на компьютере пользователя в соответствии с применяемыми в компании групповыми политиками безопасности.

4. Ответственность
Ответственность за организацию работы в дистанционном режиме возлагается на службу информационных технологий {Название Организации}.

Ответственность за соблюдение правил возлагается на всех сотрудников фирмы и третьих лиц, работающих в дистанционном режиме. Контроль выполнения и пересмотр политики возлагается на службу безопасности информации. Провести анализ

Шаблон 13

Политика использования сетевых служб

Политика сетевой безопасности в {Название Организации} представляет совокупность положений, правил и практических приемов, устанавливающих подход организации к использованию ее сетевых ресурсов и определяющих, как следует обеспечивать защиту ее сетевой инфраструктуры и сервисов.
Политика сетевой безопасности {Название Организации} включает:

- политику доступа к сетевым сервисам;
- политику реализации межсетевых экранов.

Политика доступа к сетевым сервисам определяет список сервисов Интернет, к которым пользователи должны иметь ограниченный доступ. Под сервисами Интернет будем понимать сервисы, предоставляемые в сети Интернет пользователям, программам, системам, уровням, функциональным блокам. Наиболее распространенными сервисами являются хранение данных, передача сообщений и блоков данных, электронная и речевая почта, предоставление соединений, видеосервис.
Необходимо ограничение методов доступа, чтобы пользователи не могли обращаться к «запрещенным» сервисам Интернет обходными путями. Набор обходных путей зависит от политики безопасности для данного межсетевого экрана.

Политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Правила доступа к внутренним ресурсам должны базироваться на одном из следующих принципов:

- запрещать все, что не разрешено в явной форме;
- разрешать все, что не запрещено в явной форме.

Реализация межсетевого экрана на основе обоих принципов.

Шаблон 14

Политика по работе с инцидентами информационной безопасности

Политика разработана в целях выявления, предотвращения и устранения последствий нарушений законодательства Российской Федерации в области обработки конфиденциальной информации.

1. Инциденты в области информационной безопасности возникают при нарушении правил и требований информационной безопасности.

В ходе инцидента реализуются (или создается возможность для реализации) угрозы информационной безопасности, что, как правило, приводит к нанесению вреда активам {название организации}.

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов информационных систем персональных данных.

Работа с инцидентами включает в себя 3 направления:

- выявление инцидентов в области информационной безопасности;
- реакция на инциденты в области информационной безопасности;
- предупреждение инцидентов в области информационной безопасности.

2. Выявление инцидентов в области информационной безопасности

Работа по выявлению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

- выявление инцидентов в области информационной безопасности с помощью технических средств;
- выявление инцидентов в области информационной безопасности в ходе мероприятий по контролю за обработкой персональных данных;
- выявление инцидентов с помощью персонала {название организации}.

3. Реакция на инциденты в области информационной безопасности

Реакция на инциденты в области информационной безопасности включает в себя:

- фиксацию инцидента в области информационной безопасности;
- определение границ инцидента и ущерба (в том числе потенциального) от реализации угроз информационной безопасности в ходе инцидента;
- ликвидация последствий инцидента и полное либо частичное возмещение ущерба;
- наказание виновных в инциденте информационной безопасности.

4. Предупреждение инцидентов в области информационной безопасности

Предупреждение инцидентов строится на:

- планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками {название организации};
- проведения мероприятий по обучению сотрудников {название организации} правилам и способам работы со средствами защиты информационных систем персональных данных;
- доведении до сотрудников норм законодательства в области защиты персональных данных и внутренних документов {название организации}, устанавливающих ответственность за нарушение требований информационной безопасности;
- разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимающимися на работу;

- своевременной модернизации системы обеспечения информационной безопасности информационных систем персональных данных с учетом возникновения новых угроз информационной безопасности;
- своевременном обновлении программного обеспечения, в т. ч. баз сигнатур антивирусных средств.

5. Причины инцидентов в области информационной безопасности

Причинами инцидентов в области информационной безопасности являются:

- действие враждебных интересам {название организации} организаций и отдельных лиц;
- отсутствие персональной ответственности за обеспечение информационной безопасности персональных данных сотрудников {название организации} их руководителей;
- недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности персональных данных;
- отсутствие моральной и материальной стимуляции за соблюдение правил и требований информационной безопасности;
- недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;
- совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;
- наличие привилегированных бесконтрольных пользователей в информационной системе;
- пренебрежение правилами и требованиями информационной безопасности сотрудниками {название организации};
- и другие причины.

6. Расследование инцидентов в области информационной безопасности

Расследование инцидентов в области информационной безопасности должно включать в себя:

- формирование комиссии по расследованию инцидента в области информационной безопасности;
- определение границ инцидента – информационных ресурсов, технических средств и персонала, затронутых инцидентом;
- определение причин инцидента, факторов, влияющих на возникновение инцидента;
- определение участников инцидента;
- определение последствий инцидента;
- составление заключения по результатам расследования;
- выработка рекомендаций по предотвращению возникновения подобных инцидентов в будущем.

7. Работа с персоналом по предупреждению инцидентов

Как правило, самым слабым звеном в любой системе безопасности является человек. Наличие современных доступных способов воздействия на персонал {название организации}, таких как социальная инженерия, фишинг, подмена электронных идентификаторов, номеров телефонов и т. д., делает пользователя информационной системы персональных данных частым объектом внимания злоумышленника. Поэтому направление работы с персоналом является основным направлением работы подразделений информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащие

выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.
Персонал {название организации} является так же важным источником сведений об инцидентах информационной безопасности. Поэтому необходимо донести до сотрудников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности являются поводом для смягчения либо отмены наказания за нарушение требований информационной безопасности.
Частой причиной инцидентов информационной безопасности является личная обида подчиненных на своих руководителей, либо коллег. Поэтому благоприятный микроклимат в коллективе является необходимым фактором обеспечения информационной безопасности в организации.

Шаблон 15

Политика обеспечения непрерывности ИТ-сервисов

Настоящая политика устанавливает принципы менеджмента непрерывности ИТ-сервисов в {название организации}. Процесс Управления Непрерывностью ИТ-сервисов входит в общий Процесс Менеджмента Непрерывностью Бизнеса (МНБ).
Политика МНБ определяет следующие процессы:

- организационную деятельность по установлению способности к непрерывности бизнеса;
- непрерывный менеджмент и поддержку способности к обеспечению непрерывности бизнеса.

1. **Организационная деятельность** включает в себя установление требований и полного цикла непрерывности бизнеса от проектирования, построения, внедрения до первоначального применения проверки способности организации к непрерывности бизнеса.

2. **Непрерывная поддержка и менеджмент** включают в себя: внедрение непрерывности бизнеса в организации; проведение регулярных учений по применению планов обеспечения непрерывности бизнеса; актуализацию и обмен информацией в соответствии с этим планом, особенно, если происходят существенные изменения в производственных площадях, персонале, организационной структуре, производственных и технологических процессах или рыночных условиях.

3. Цели применения

Политика в области МНБ должна соответствовать природе, масштабу, сложности, географии и критичности видов деятельности организации, отражать ее культуру, взаимосвязанные области и деловую среду. Политика в области МНБ определяет требования к процессу обеспечения непрерывности бизнеса и должна обеспечивать соответствие действий в области непрерывности бизнеса потребностям организации в случае возникновения инцидента, а также развитие способности организации к непрерывности бизнеса. Способность к МНБ должна быть интегрирована в деятельность организации по управлению изменениями таким образом, чтобы способность к непрерывности бизнеса способствовала росту номенклатуры продукции и объема услуг.

4. Основные положения политики непрерывности бизнеса

Политика в области непрерывности бизнеса должна обеспечивать организации документированные принципы и цели, к которым должна стремиться организация и, на соответствие которым, необходимо проводить измерение способности к непрерывности бизнеса. Политика в области МНБ утверждается руководителем организации {название организации}, например, генеральным директором или председателем совета директоров.

В области МНБ организацией {название организации} определены:

- области применения МНБ в организации;
- необходимые ресурсы для МНБ;
- принципы, руководящие указания и минимальное количество стандартов организации в области МНБ;
- ссылки на соответствующие стандарты, инструкции или другие нормативные акты организации, которые должны быть включены в документы или могут быть использованы как точки отсчета.

Организация {название организации} должна поддерживать в рабочем состоянии политику, стратегии, планы и решения в области МНБ и проводить их анализ через запланированные интервалы времени в соответствии с потребностями организации.

5. Распределение ответственности и полномочий

Высшее руководство организации {название организации} должно назначить:

- лицо из числа высшего руководства, наделенное соответствующими полномочиями, ответственное за политику в области МНБ и ее внедрение;
- одного или несколько лиц, ответственных за выполнение и поддержку программы МНБ.

Обязанности, подотчетность, ответственность и полномочия персонала должны быть установлены в рабочих и должностных инструкциях.

Анализ этих обязанностей необходимо проводить в процессе аудита организации.

Надлежащее выполнение обязанностей в области обеспечения непрерывности бизнеса может быть усилено путем их включения в политику организации в области аттестации, компетентности и поощрения персонала.

6. Осуществление непрерывности бизнеса в организации

Деятельность по выполнению программы непрерывности бизнеса должна включать в себя проектирование, разработку и внедрение программы.

Организация должна осуществлять следующие действия:

- обмен информацией о программе с причастными сторонами;
- организацию и/или обеспечение соответствующего обучения персонала;
- проведение учений по обеспечению непрерывности бизнеса (см. раздел 9).

5.3.2 Организация может адаптировать признанные методы менеджмента для обеспечения эффективного управления программой непрерывности бизнеса.

13. Порядок действий сотрудников (персонала) банка и перечень мероприятий, которые должны быть выполнены в момент и после возникновения нестандартных и чрезвычайных ситуаций

Порядок действий сотрудников (персонала) головного офиса банка и перечень мероприятий, которые должны быть выполнены в момент и после возникновения нестандартных и чрезвычайных ситуаций, определён приложениями к настоящей политике с учётом особенности и причин возникновения нестандартных и чрезвычайных ситуаций.

Шаблон 16

Политика обеспечения восстановления

В Учреждении должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес-процессов.

В каждом плане поддержки непрерывности бизнеса должны быть чётко указаны условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.

Для каждого плана должен быть назначен определённый владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

План восстановления определён приложением к настоящей политике.

Шаблон 17

Предоставление услуг сторонним организациям

1. Соглашения о предоставлении услуг.

В соглашения о предоставлении услуг {Название Организации} сторонним организациям должны быть включены требования безопасности, описание, объёмы и характеристики качества предоставляемых услуг.

2. Анализ предоставления услуг

Услуги, отчёты и записи, предоставляемые {Название Организации} сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

- контроль объёма и качества услуг, оговоренных в соглашениях;

- предоставление сторонней организации информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
- анализ предоставленных сторонними организациями отчётов о предоставленных услугах;
- управление любыми обнаруженными проблемами.

3. Приёмка систем

В {Название Организации} должен быть разработан и утверждён порядок приёмки новых ИС, обновления и новых версий ПО.

ПРИЛОЖЕНИЕ Е

Оформлене акта классификации информационных систем.

Утверждаю
Руководитель предприятия
"_____"_____"_____"г.

АКТ

классификации информационной системы обработки информации

XXXXXXXXXXXXXXXX

(наименование информационной системы)

Комиссия, в соответствии с приказом от "_____"_____"_____"г.	N____	в составе:
председатель: Xxxxxxxxxxxx X.X.		
члены комиссии: Xxxxxxxxxxxxx X.X. Xxxxxxxxxxxxx X.X. Xxxxxxxxxxxxx X.X.		

провела классификацию информационной системы

_____XXXXXXXXXXXXXXXX_____,

(наименование информационной системы)

рассмотрев исходные данные на автоматизированную систему обработки информации (АС) наименование автоматизированной системы условия ее эксплуатации (многопользовательский, однопользовательский; с равными или разными правами доступа к информации {выбрать нужное}), с учетом характера обрабатываемой информации (служебная тайна, коммерческая тайна, персональные данные и т.д. {выбрать нужное}) и в соответствии с руководящими документами Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации,

РЕШИЛА:

Установить АС *наименование автоматизированной системы*

класс _XX_.

Председатель _____ Xxxxxxxxxxxx X.X.

Члены комиссии _____ Xxxxxxxxxxxx X.X.

_____ Xxxxxxxxxxxx X.X.

_____ Xxxxxxxxxxxx X.X.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

ПРИЛОЖЕНИЕ Ж

Условные обозначения к планировкам выделенных помещений

Обозначение	Наименование
	Граница контролируемой зоны

Таблица. Характеристики конструкций

№ варианта	Стены	Дверь	Окно
1	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 1,5 кирпича	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 3,0 мм
2	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 2 кирпича	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: с уплотняющими прокладками	Одинарное остекление без уплотнительных прокладок, толщина 4,0 мм
3	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 2,5 кирпича	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 2,5 см из 3 мм фанеры без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 6,0 мм
4	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 2 кирпича	-	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 3,0/3,0
5	Стена из пустотелого кирпича, толщина 380,0 мм	-	Двойное остекление, расстояние между стеклами 57 мм, со звукопоглощающим материалом, толщина 3,0/3,0
6	Стена из пустотелого кирпича, толщина 510,0 мм	Глухая щитовая дверь, толщиной 40 мм, облицованная с двух сторон фанерой, толщиной 4 мм: С уплотняющими прокладками	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала, толщина 3,0/3,0
7	Стена из железобетона, толщина 160,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным	-

		стекловатой: Без уплотняющих прокладок	
8	Стена из железобетона, толщина 180,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой: С уплотняющими прокладками	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 4,0/4,0
9	Стена из железобетона, толщина 160,0 мм	-	Двойное остекление, расстояние между стеклами 57 мм, со звукопоглощающим материалом, толщина 4,0/4,0
10	Стена из железобетона, толщина 200,0 мм	-	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала, толщина 4,0/4,0
11	Стена из железобетона, толщина 300,0 мм	-	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 6,0/3,0
12	Стена из железобетона, толщина 800,0 мм	-	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала, толщина 6,0/3,0
13	Газобетонная плита, толщина 240,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: без уплотняющих прокладок	-
14	Газобетонная плита, толщина 240,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: с	Двойное остекление, расстояние между стеклами 190 мм, без