ГОСЭКСПЕРТИЗА
Челябинской области

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ «УПРАВЛЕНИЕ ГОСУДАРСТВЕННОЙ ЭКСПЕРТИЗЫ ПРОЕКТНОЙ ДОКУМЕНТАЦИИ, ПРОЕКТОВ ДОКУМЕНТОВ ТЕРРИТОРИАЛЬНОГО ПЛАНИРОВАНИЯ И ИНЖЕНЕРНЫХ ИЗЫСКАНИЙ ЧЕЛЯБИНСКОЙ ОБЛАСТИ»
ОГАУ «ГОСЭКСПЕРТИЗА ЧЕЛЯБИНСКОЙ ОБЛАСТИ»

УТВЕРЖДЕНО

Приказом начальника
ОГАУ «Госэкспертиза Челябинской области» Грищенко О.В.

от «14» октября 2022 г. № 326

ПОЛИТИКА
информационной безопасности
ОГАУ «Госэкспертиза Челябинской области»

Челябинск, 2022

Оглавление

1. Обозначения и сокращения 3
2. Общие положения 5
3. Доступ пользователей 7
4. Управление идентификаторами и паролями 9
5. Использования ИР 11
6. Использование ПО 11
7. Использование АРМ и ИС 13
8. Обработка конфиденциальной информации 15
9. Использование электронной почты 15
10. Работа в сети Интернет 18
11. Использование носителей информации 19
12. Защита от вредоносного ПО 20
13. Сетевая безопасность 21
14. Физическая безопасность 23
15. Дублирование, резервное копирование и хранение информации 24
16. Криптографические средства 24
17. Аудит информационной безопасности 26
18. Классификация информации 27
19. Соблюдение законодательства и данной политики 29
20. Заключение 30

1. Обозначения и сокращения

1.1. Сокращения:

- АРМ – автоматизированное рабочее место;
- ИБ – информационная безопасность;
- ИС – информационная система;
- ИР – информационный ресурс;
- МЭ – межсетевой экран;
- НДВ – не декларированные возможности;
- НСД – несанкционированный доступ;
- ОС – операционная система;
- ПДн – персональные данные;
- ПО – программное обеспечение;
- СЗИ – средства защиты информации;
- СКЗИ – средства криптографической защиты информации;
- СУИБ – Система управления информационной безопасностью.

1.2. Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

1.3. Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

1.4. Безопасность информации – защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.

1.5. Бизнес-процесс – последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Учреждения.

1.6. Закрытый ключ подписи – уникальная последовательность символов, известная владельцу сертификата и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств ЭЦП.

1.7. Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

1.8. Идентификация – присвоение субъектам доступа, объектам доступа

идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

1.9. Информационная безопасность – состояние защищённости интересов Учреждения.

1.10. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.11.Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

1.12. Носитель ключевой информации (ключевой носитель) – материальный носитель информации, содержащий закрытый ключ подписи или шифрования.

1.13. Открытый ключ подписи – уникальная последовательность символов, соответствующая закрытому ключу подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения подлинности ЭЦП в электронном документе.

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

1.15. Привилегии – это права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.

1.16. Риск – сочетание вероятности события и его последствий.

1.17. Сертификат ключа подписи (сертификат) – документ на бумажном носителе или электронный документ, который включает в себя открытый ключ ЭЦП и который выдается удостоверяющим центром для подтверждения подлинности ЭЦП и идентификации владельца сертификата.

1.18. Суперпользователь – администратор ИС, имеющий право на выполнение всех без исключения операций.

1.19. Угроза – Опасность, предполагающая возможность потерь (ущерба).

1.20. Учреждение – ОГАУ «Госэкспертиза Челябинской области».

1.21. Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

1.22. Шифрование – способ защиты информации от несанкционированного доступа за счет ее обратимого преобразования с использованием одного или нескольких ключей.

1.23. Электронная цифровая подпись (ЭЦП) – реквизит электронного

документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации и позволяющий идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе.

2. Общие положения

2.1. Политика информационной безопасности Учреждения (далее – Политика) разработана в соответствии с требованиями действующего законодательства и нормативных актов Российской Федерации: Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», № 63-ФЗ «Об электронной подписи», Федерального закона от 6 апреля 2011 г.

2.2. Предметом настоящей Политики является:

- порядок доступа;
- управление паролями;
- сетевая безопасность;
- локальная безопасность;
- физическая безопасность (доступ в помещения);
- обеспечение защиты персональных данных;
- дублирование, резервирование и хранение информации;
- ответственность за соблюдение положений Политики ИБ.

2.3. Концептуальная схема информационной безопасности Учреждения направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

2.4. Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Учреждении функции обеспечения ИБ возложены на Службу контроля, развития, сопровождения (далее – Служба) со следующими задачами и функциями:

- разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности;
- оказание методической помощи сотрудникам в вопросах обеспечения ИБ;
- выявление, оценка и прогнозирование угроз информационной безопасности;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;
- проведение периодического контроля состояния ИБ, учет и анализ результатов с выработкой решений по устранению уязвимостей и нарушений;
- контроль за использованием закрытых каналов связи и ключей с цифровыми подписями;
- организация плановых проверок режима защиты, и разработка соответствующей документации, анализ результатов, расследование нарушений;
- разработка и осуществление мероприятий по защите персональных данных;
- обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений;
- организация взаимодействия со всеми структурами, участвующими в их обработке, выполнение требований законодательства к информационным системам персональных данных, контроль действий операторов, отвечающих за их обработку.

2.5. Организационно-правовой статус сотрудников Службы контроля, развития, сопровождения:

- сотрудники имеют право беспрепятственного доступа во все помещения, где установлены технические средства с Информационными системами;
- сотрудники имеют право получать от пользователей необходимую информацию по вопросам применения информационных технологий, в части касающейся вопросов информационной безопасности;
- Специалист Службы, назначенный ответственными за системное администрирование (далее – Системный администратор), имеет право проводить аудит действующих и вновь внедряемых ИС, ПО, на предмет реализации требований защиты и обработки информации, соответствию требований законодательства, запрещать их эксплуатацию, если не отвечают требованиям или продолжение эксплуатации может привести к серьезным последствиям в случае реализации значимых угроз безопасности;
- сотрудники имеют право контролировать деятельность пользователей по вопросам обеспечения ИБ;

- сотрудники имеют право готовить предложения руководству по обеспечению требований ИБ.

2.6. Требования настоящей Политики распространяются на всех сотрудников Учреждения (штатных, временных, работающих по договору подряда и т.п.).

2.7. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах с контрагентами.

3. Доступ пользователей

3.1. Управление доступом к внутренним (корпоративным) сервисам реализовано с помощью штатных средств (операционных систем MS Windows, Linux и используемых ими СУБД) в целях идентификации и проверки подлинности субъектов доступа при входе, а также для их регистрации входа (выхода) в сервисы (из сервисов).

3.2. Требование идентификации и аутентификации при входе в информационную систему определяется приказом ФСТЭК № 21 от 18.02.2013г.

3.3. В составе ИСПДн используются сертифицированные или разрешенные к применению ФСТЭК средства защиты информации от НСД.

3.4. Все действий пользователей регистрируются в журналах событий системного и прикладного ПО. Данные электронные журналы доступны для чтения, анализа и резервного копирования только Системному администратору, который несет персональную ответственность за полноту и точность отражения в журнале имевших место событий.

3.5. Запрещается доступ суперпользователей к серверам и базам данных под единой или предопределенной учетной записью.

3.6. Любой доступ к базам данных без фиксации в соответствующих журналах или лог-файлах запрещен.

3.7. В случае увольнения сотрудника, имеющего права суперпользователя, пароли доступа к серверам и базам данных меняются в тот же день.

3.8. Основными пользователями информации в информационной системе Учреждения являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

3.9. Доступ сотрудника к информационным ресурсам Учреждения должен быть санкционирован руководителем структурного подразделения, в котором

числится согласно штатному расписанию данный сотрудник.

3.10. Каждому пользователю, допущенному к работе с конкретным информационным активом Учреждения, выдаются Идентификатор (логин или учетная запись) и пароль.

3.11. 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 90 дней;
- 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 (сотрудники Службы контроля, развития, сопровождения);
- 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.

3.12. Наделение привилегиями и их использование должно быть строго ограниченным и управляемым:

- 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, для выполнения функциональных обязанностей сотрудников;
- должен быть обеспечен процесс санкционирования всех предоставленных

привилегий и создание отчетов по ним, привилегии нельзя предоставлять до завершения процесса их регистрации;

- необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;

- уникальные привилегии должны присваиваться на другой ID пользователя, не тот, который используется при обычной работе пользователя.

3.13. Повышение привилегий администратором для ранее существовавших учетных записей или создание новых административных групп согласовывается с руководством Учреждения.

3.14. Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Учреждения осуществляется в процессе аудита ИБ.

4. Управление идентификаторами и паролями

4.1. Идентификатор (логин или учетная запись) и пароль пользователя в ИС или корпоративному сервису 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.

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

4.3. 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, использование общей учётной записи должно однозначно идентифицировать текущего владельца учётной записи в каждый момент времени (сообщение-запрос по электронной почте Системному администратору об использовании учетной записи).

4.4. Идентификаторы и пароли к ИС и к информационным активам выдаются специалистами Службы контроля, развития, сопровождения.

4.5. Предоставление логинов и паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

- все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых логинов и паролей;

- необходимо избегать передачи логинов и паролей с использованием третьих лиц или незашифрованной электронной почтой;

- идентификаторы и пароли должны храниться в электронном виде только в защищенной форме;

- длина пароля должна быть не менее 8 и не более 14 символов, пароль должен состоять из букв латинского алфавита (A-z), арабских цифр (0-9), буквенная часть пароля должна содержать как строчные, так и прописные (заглавные) буквы;
- необходимо изменять пароли пользователей не реже одного раза в 180 дней.

4.6. Пароль не должен содержать легко вычисляемые сочетания символов:

- имена, фамилии, номера телефонов, даты;
- последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.);
- общепринятые сокращения («USER», «TEST» и т.п.);
- повседневно используемое слово, например, имена или фамилии друзей, коллег, актёров или сказочных персонажей, клички животных;
- компьютерный термин, команда, наименование компаний, web сайтов, аппаратного или программного обеспечения;
- что-либо из вышеперечисленного в обратном написании;
- что-либо из вышеперечисленного с добавлением цифр в начале или конце.

4.7. Сотруднику запрещается:

- сообщать свой идентификатор и пароль кому-либо;
- указывать пароль в сообщениях электронной почты;
- хранить учетные данные, 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 и сервисам.

4.8. При необходимости можно рассмотреть возможность использования других технологий идентификации и аутентификации пользователей, в частности, проверки ЭЦП и аппаратных средств.

4.9. Сотрудник обязан:

- в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации сотруднику Службы контроля, развития, сопровождения;
- немедленно сообщить сотруднику Службы контроля, развития, сопровождения в случае получения от кого-либо просьбы сообщить пароль;
- менять пароль по требованию сотрудников Службы контроля, развития,

сопровождения.

4.10. 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. Использования ИР

5.1. Общие обязанности пользователя:

- при работе с ПО руководствоваться нормативной документацией (инструкциями пользователя);
- обращаться в службу поддержки пользователей или к специалистам, назначенными ответственными за системное администрирование и информационную безопасность (Служба контроля, развития, сопровождения), 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.

5.2. К работе в ИС и ИР Учреждения допускаются лица, назначенные на соответствующую должность и ознакомленные с настоящей Политикой.

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

5.4. Для выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим ИР. ИР являются каталоги и файлы, хранящиеся на дисках серверов Учреждения, базы данных, электронная почта.

5.5. Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы.

6. Использование ПО

6.1. На АРМ Учреждения допускается использование только лицензионного ПО, включенного в перечень разрешённого в Учреждении ПО.

6.2. Решение о приобретении и установке ПО, необходимого для реализации задач, поставленных перед Учреждением, принимает Начальник Учреждения по представлении Заместителя начальника Учреждения по вопросам контроля, развития, сопровождения.

6.3. Документы, подтверждающие покупку ПО, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся у Системного администратора Службы контроля, развития, сопровождения.

6.4. Пользователи АРМ самостоятельно не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ Учреждения. Указанные работы, а также работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только сотрудниками Службы контроля, развития, сопровождения.

6.5. Сведения о вновь приобретённом ПО должны быть внесены в перечень разрешённого в Учреждении ПО.

6.6. С целью обеспечения ИБ на всех АРМ установлено специализированное ПО, позволяющее контролировать и фиксировать все события в локальной и удаленной сети, а также все каналы передачи данных, осуществлять мониторинг активности и мониторинг веб-трафика.

6.7. На каждом АРМ, или сервере при вводе в эксплуатацию или после переустановки ОС сотрудниками Службы контроля, развития, сопровождения в обязательном порядке устанавливается и активируется антивирусная программа. Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на АРМ, серверах, осуществляется специалистами Службы контроля, развития, сопровождения в соответствии с руководствами по применению конкретных антивирусных средств.

6.8. Исходя из требований ФСТЭК от 30 июля 2012 г. № 240/24/3095 к средствам антивирусной защиты антивирусное ПО должно соответствовать 6 классу защиты и типу «А» для применения в информационных системах персональных данных 4 класса.

6.9. Антивирусная защита предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей Учреждения.

6.10. Отключение или не обновление антивирусных средств не допускается. Установка и обновление антивирусных средств в организации контролируется централизованно Системным администратором Службы контроля, развития, сопровождения.

6.11. Система обнаружения атак, встроенная в антивирусную программу, сохраняет информацию об атаках и подозрительной активности в лог-файлы,

которые анализирует Системный администратор Службы контроля, развития, сопровождения.

6.12. В случае массированной вирусной атаки сотрудники Службы контроля, развития, сопровождения определяют масштаб заражения, принимают меры к локализации, блокированию распространения, определяют источник заражения, характер действия и распространения вируса, нейтрализуют последствия атаки. При необходимости ставятся патчи и необходимые обновления ПО, закрывающие уязвимости, используемые вирусами.

7. Использование АРМ и ИС

7.1. Каждый сотрудник Учреждения, обеспеченный АРМ, получает персональное сетевое имя, пароль, адрес электронной почты и личный каталог в сети, который предназначен для хранения рабочих файлов.

7.2. Все АРМ, установленные в Учреждении, имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией. Изменение установленной конфигурации возможно по служебной записке на Начальника учреждения, согласованной Службой контроля, развития, сопровождения. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется Службой контроля, развития, сопровождения.

7.3. Запрещено хранение на жестких дисках АРМ Учреждения игр, фильмов и прочих материалов, развлекательного характера, не относящихся к исполнению своих должностных обязанностей.

7.4. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в Службу контроля, развития, сопровождения.

7.5. Сотрудники Службы контроля, развития, сопровождения имеют право осуществлять контроль над установленным на компьютере программным обеспечением, и принимать меры по ограничению возможностей несанкционированной установки программ.

7.6. Передача документов внутри Учреждения в электронном виде производится только посредством общих папок, а также средствами электронной почты.

7.7. 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 Службу контроля, развития, сопровождения о любых фактах нарушения требований ИБ;
- ставить в известность отдел Службы контроля, развития, сопровождения о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;
- незамедлительно выполнять предписания Службы контроля, развития, сопровождения Учреждения;
- предоставлять АРМ сотрудникам отдела Службы контроля, развития, сопровождения для контроля;
- при необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;
- в случае необходимости продолжения работы в нерабочие дни проинформировать об этом Службу контроля, развития, сопровождения.

7.8. При использовании ИС Учреждения запрещено:

- отключать средства управления и средства защиты, установленные на АРМ;
- передавать конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным;
- передавать информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;
- передавать угрожающую, клеветническую, непристойную информацию;
- самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС Учреждения;
- предоставлять сотрудникам Учреждения (за исключением сотрудников Службы контроля, развития, сопровождения) и третьим лицам доступ к своему АРМ;
- запускать на АРМ ПО, не входящее в перечень разрешенного в Учреждении к использованию ПО;
- защищать информацию, способами, не согласованными со Службой контроля, развития, сопровождения заранее;
- самостоятельно подключать АРМ 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.

7.9. Все действия на АРМ и информация о посещаемых ресурсах протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Начальнику Учреждения.

8. Обработка конфиденциальной информации

8.1. При обработке конфиденциальной информации сотрудники обязаны:

- применять средства защиты от неавторизованного доступа при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети Учреждения;
- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;
- 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;

8.2. Документы и носители с конфиденциальной информацией должны убираться сотрудниками в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.

8.3. АРМ должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра. Заблокировать компьютер можно, используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер».

8.4. Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги.

8.5. При использовании мобильных средств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Учреждению.

9. Использование электронной почты

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

сообщений и документов в электронном виде.

9.2. 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.

9.3. Организацией и обеспечением порядка работы электронной почты в Учреждении занимается Служба контроля, развития, сопровождения.

9.4. Каждый сотрудник Учреждения получает почтовый адрес вида инициалы@ge74.ru в домене Учреждения. Адрес электронной почты выдаётся сотрудником Служба контроля, развития, сопровождения при начальной регистрации пользователя в домене Учреждения.

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

9.6. 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.

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

9.8. 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.

9.9. 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.

9.10. 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.

9.11. 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.

9.12. Использование сообщений корпоративной электронной почты в интересах Учреждения, в том числе ознакомление с содержанием сообщений, осуществляется только Системным администратором Службы контроля, развития, сопровождения по непосредственному запросу Начальника Учреждения.

9.13. Исходящие электронные сообщения сотрудников Учреждения должны содержать следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (вложенные файлы);
- подпись отправителя.

9.14. Формат подписи отправителя:

С уважением,

<Фамилия Имя Отчество>

<Должность>

<Структурное подразделение>

<Наименование Учреждения>

<Телефон>

<Адрес электронной почты>

<Сайт>

<Адрес>

9.15. Отказ от дальнейшего предоставления сотруднику Учреждения услуг электронной почты может быть вызван нарушениями требований настоящей Политики.

9.16. Прекращение предоставления сотруднику Учреждения услуг электронной почты наступает при прекращении действия трудового договора (договора подряда) сотрудника.

10. Работа в сети Интернет

10.1. Доступ к сети Интернет предоставляется сотрудникам Учреждения в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к информационным ресурсам и ИС.

10.2. Для доступа сотрудников Учреждения к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.

10.3. При использовании сети Интернет необходимо:

- соблюдать требования настоящей Политики;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность Службу контроля, развития, сопровождения о любых фактах нарушения требований настоящей Политики;

10.4. При использовании сети Интернет запрещено:

- использовать предоставленный Учреждением доступ в сеть Интернет в личных целях;
- посещать социальные сети, просматривать и скачивать медиаконтент, игры и т.п., не связанные с выполнением своих должностных обязанностей;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Учреждения;
- использовать облачные сервисы на рабочих местах сотрудников, обрабатывающих информацию конфиденциального характера;
- публиковать, загружать и распространять материалы содержащие:

  - конфиденциальную информацию, а также информацию, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с Системным администратором Службы контроля, развития, сопровождения;

- 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.

10.5. 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.

10.6. 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.

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

11. Использование носителей информации

11.1. Под использованием носителей информации в Учреждения понимается их подключение к инфраструктуре и корпоративным ресурсам с целью обработки, приёма/передачи информации между ИС и носителями информации.

11.2. При использовании сотрудниками личных носителей информации к носителям предъявляются те же требования ИБ, что и для стационарных АРМ. Целесообразность дополнительных мер обеспечения ИБ определяется Службой контроля, развития, сопровождения.

11.3. Перед любым взаимодействием (обработкой, приёмом\передачей информации) носителей информации и ИС, такие носители подлежат обязательной проверке на отсутствие вредоносного ПО.

11.4. При использовании носителей информации, сотрудник обязан:

- соблюдать требования настоящей Политики;
- использовать носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность Службу контроля, развития, сопровождения о любых фактах нарушения требований настоящей Политики.

11.5. При использовании носителей информации пользователям запрещено:

- использовать носители информации в личных целях;
- использовать носители информации, не прошедшие обязательную проверку на отсутствие вредоносного ПО;
- передавать носители информации с конфиденциальной информацией другим лицам (за исключением сотрудников Службы контроля, развития, сопровождения);
- оставлять носители информации с конфиденциальной информацией без присмотра, если не предприняты действия по обеспечению их физической безопасности.

11.6. Информация об использовании сотрудниками Учреждения носителей информации в ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также руководству Учреждения. Учреждение оставляет за собой право блокировать или ограничивать использование носителей информации в целях соблюдения требований ИБ.

12. Защита от вредоносного ПО

12.1. Служба контроля, развития, сопровождения регулярно проверяет сетевые ресурсы Учреждения антивирусным ПО и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

12.2. 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 Службу контроля, развития, сопровождения. После чего Системный администратор Службы контроля, развития, сопровождения должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

12.3. В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения заражения Службу контроля, развития, сопровождения, а также владельца файла и смежные подразделения, использующие эти файлы в работе.
- специалисты Службы контроля, развития, сопровождения совместно с владельцем зараженных вирусом файлов провести анализ необходимости

дальнейшего их использования.

12.4. Для предупреждения вирусного заражения рекомендуется:

- никогда не открывать файлы и не выполнять макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя. Удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;
- удалять спам, рекламу и другие бесполезные сообщения;
- никогда не загружать файлы и программное обеспечение из подозрительных или неизвестных источников, в том числе с носителей информации, полученных от третьих лиц;
- периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте.

13. Сетевая безопасность

13.1. Доступ из Интернет во внутреннюю сеть Учреждения обеспечивается на основе зарегистрированных персональных учетных записей, с использованием технологии VPN, других протоколов шифрования.

13.2. Допускается использование программ удаленного администрирования, но по согласованию с сотрудником Службы контроля, развития, сопровождения для удаленной настройки ПО на ограниченное время.

13.3. Настройка и конфигурация средств обнаружения вторжений, должны обеспечивать оперативное обнаружение несанкционированного доступа к ресурсам сети для принятия мер блокирования проникновения нейтрализации последствий.

13.4. При администрировании удаленного доступа к ресурсам корпоративной сети Учреждения предъявляются следующие требования:

- доступ предоставляется сроком на ограниченный срок с разрешения Начальника Учреждения;
- список сотрудников, которым предоставлен удаленный доступ, поддерживается в актуальном состоянии Системным администратором Службы контроля, развития, сопровождения и предоставляется по запросу Руководству Учреждения.

13.5. В целях обеспечения безопасности и нормального функционирования компьютерных сетей запрещается:

- самовольно подключать компьютерное оборудование (беспроводные точки доступа, маршрутизаторы, компьютеры и др.) к сети Учреждения и присваивать ему сетевое имя и адрес неуполномоченными на то сотрудниками;
- перемещать компьютеры между сетевыми розетками и другими

коммуникационными устройствами;

- использовать информационные ресурсы Учреждения для сетевых игр, распространения коммерческой рекламы, организации спама;
- сканировать узлы сети неуполномоченными на то сотрудниками.

13.6. Доступ через беспроводную сеть разрешается только к общедоступным ресурсам сети. Беспроводные точки устанавливает и администрирует Системный администратор Службы контроля, развития, сопровождения.

13.7. На межсетевом экране заводится лог-файл, куда записываются все обращения к ресурсам (попытки создания соединений). Доступ к лог-файлам имеет Системный администратор Службы контроля, развития, сопровождения.

13.8. Системный администратор Службы контроля, развития, сопровождения ведет протоколирование и регулярный мониторинг доступа, контролирует содержание трафика, проводит анализ лог-файлов.

13.9. Системный администратор Службы контроля, развития, сопровождения должен иметь независимый доступ к элементам системы защиты для контроля настроек конфигураций, просмотра системных журналов.

13.10. Для анализа защищенности ИС Системным администратором Службы контроля, развития, сопровождения проводится выявление и анализ уязвимостей и несоответствия в настройках ОС, ПО, СУБД, сетевого оборудования. Выявленные уязвимости протоколируются устраняются в установленные сроки.

13.11. Для обеспечения ИБ в ИС запрещается использовать ПО снятое с поддержки, имеющее уязвимости, с просроченными сертификатами.

13.12. Доступ из одного сегмента сети в другой ограничивается и разделяется маршрутизаторами. Настройкой маршрутизаторов занимается Системный администратор Службы контроля, развития, сопровождения.

13.13. Приобретение и установка средств и систем защиты ИС осуществляются по согласованию с Начальником Учреждения по инициативе Системного администратора Службы контроля, развития, сопровождения.

13.14. Передача информации конфиденциального характера (финансовые, бухгалтерские документы) за периметр сети осуществляется только по защищенным каналам. Защищенные каналы строятся с использованием криптозащиты, на базе решений VipNet, VPN, Банк-клиент или других, сертифицированных ФСТЭК.

13.15. Криптографическая защита предназначена для исключения НСД к защищаемой информации, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

13.16. Криптографическая защита реализуется путем внедрения

криптографических программно-аппаратных комплексов КриптоПро.

13.17. Все экземпляры КриптоПро должны иметь лицензию и регистрируются в Журнале СКЗИ у Системного администратора Службы контроля, развития, сопровождения.

13.18. Электронные подписи выдаются удостоверяющим центром на определенное должностное лицо, по его документам на основании заключенного договора. Инициатором заключения договора является структурное подразделение. После получения ключа ЭП, снимается копия сертификата и регистрируется в журнале учета СКЗИ у Системного администратора Службы контроля, развития, сопровождения.

13.19. Носители ключей ЭП должны храниться в запираемых на ключ местах либо сейфах ответственных лиц. Доступ неуполномоченных лиц к носителям ключей должен быть исключен. Передача ключей запрещена.

13.20. Запрещается оставлять носители с ЭП, установленными в компьютер, при покидании рабочего места.

13.21. Компьютеры, на которых установлены средства криптозащиты, должны соответствовать требованиям, изложенным в документации по КриптоПро.

14. Физическая безопасность

14.1. Все объекты критичные с точки зрения ИБ (сервера баз данных, маршрутизаторы, ИБП, МЭ и т.д.) находятся в контролируемых зонах – помещение серверной.

14.2. Сотрудники Службы контроля, развития, сопровождения несут ответственность за помещение серверной и имеют непосредственный доступ к ней:

- ключ от серверной находится у Системного администратора Службы контроля, развития, сопровождения в 1 экземпляре и Секретаря учреждения в 1 экземпляре, и хранятся в шкафах, исключаемых несанкционированный доступ к ним;
- дверь серверной должна всегда находится в закрытом на замок состоянии;
- при необходимости доступ в серверную к оборудованию третьим лицам может быть обеспечен при нахождении сотрудника Службы контроля, развития, сопровождения в серверной на все время работ.

14.3. При неавтоматизированной обработке информации конфиденциального характера документы (личные дела сотрудников, карточки лицевых счетов, картотека и т.д.) должны храниться в шкафах или сейфах, исключаемых несанкционированный доступ к ним.

14.4. В контролируемых зонах Учреждения ведется видеонаблюдение.

14.5. Входные и межэтажные двери 5 и 6 этажей оборудованы системой контроля доступа. Системный администратор Службы контроля, развития, сопровождения осуществляет администрирование данной системы, в том числе выдачу, замену, изъятие и аннулирование карт доступа по служебной записке начальников структурных подразделений.

14.6. Доступ к специалистам 5 этажа ограничен для третьих лиц. Клиенты Учреждения могут попасть к экспертам Учреждения только по предварительной записи в соответствии с установленными днями приема только в сопровождении непосредственного специалиста.

14.7. В случае увольнения (выбытия на длительное время) сотрудников Учреждения Начальник отдела правовой и кадровой работы должен изъять карту доступа и поставить в известность Системного администратора Службы контроля, развития, сопровождения.

14.8. В здании офиса Учреждения действует пропускной режим на вахте 1 этажа основного здания.

14.9. Дверь на 6 этаже Учреждения оборудована домофоном, открытие двери осуществляет Секретарь.

15. Дублирование, резервное копирование и хранение информации

15.1. Для обеспечения физической целостности данных, во избежание умышленного или неумышленного уничтожения или искажения защищаемой информации и конфигураций информационных систем организуется резервное копирование баз данных, конфигураций, файлов настроек, конфигурационных файлов.

15.2. Для обеспечения гарантированного восстановления особо важной информации, которая может быть утеряна вследствие аппаратных сбоев, воздействия вирусов-шифровальщиков производится ежедневное резервное копирование содержимого дисков файловых серверов.

15.3. Ответственными за организацию резервного копирования, хранения копий и восстановления информации являются специалисты Службы контроля, развития, сопровождения.

16. Криптографические средства

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

16.2. 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.

16.3. 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.

16.4. 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.

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

16.6. 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.

16.7. 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.

16.8. ЭЦП обеспечивают защиту аутентификации и целостности электронных документов.

16.9. 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).

16.10. 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.

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

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

17. Аудит информационной безопасности

17.1. Учреждение должно проводить внутренние проверки СУИБ через запланированные интервалы времени.

17.2. Основные цели проведения таких проверок:

- оценка текущего уровня защищённости ИС;
- выявление и локализация уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИР;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

17.3. В число задач, решаемых при проведении проверок и аудитов СУИБ, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

17.4. Руководство и сотрудники Учреждения при проведении у них аудита СУИБ обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

17.5. В целях поддержания ИБ, Учреждение следует рекомендациям, утвержденным Министерством информационных технологий. Так же следует поддерживать ИБ, согласно трендам в этой сфере.

18. Классификация информации

18.1. Предлагаемая система классификации делит информацию на четыре класса. Самый низкий, первый, наименее секретный, а наивысший, четвёртый, предназначен для самых важных данных и процессов. Каждый класс включает в себя требования предыдущего. Например, если система соответствует третьему классу, то она должна следовать требованиям первого, второго и третьего классов. Если в системе есть данные по более чем одному классу, то вся система классифицируется по наивысшему классу содержащейся информации.

18.2. Класс 1: Публичная/несекретная информация.

Описание:

Данные в этих системах могут быть доступны широкому кругу лиц без ущерба для учреждения (т. е. данные не конфиденциальны). Целостность данных не является жизненно важной. Прекращение обслуживания из-за атаки - приемлемый риск. Примеры: тестовые сервисы без секретной информации, некоторые справочные службы.

Требования к хранению: отсутствуют.

Требования к передаче: отсутствуют.

Требования к уничтожению: отсутствуют.

18.3. Класс 2. Внутренняя информация.

Описание:

Доступ извне к этим данным должен быть ограничен, но последствия в случае их разглашения некритичны (т. е. учреждение может оказаться в неловком положении). Доступ внутри учреждении регламентирован. Целостность данных важна, но не жизненно. Примеры таких данных можно встретить у разработчиков (отсутствие реальных данных), в некоторых общественных сервисах, клиентских данных, «обычных» рабочих документах, протоколах собраний и внутренних телефонных книгах.

Требования к хранению:

ИТ системы, восприимчивые к вирусным атакам, должна регулярно сканироваться на предмет обнаружения вирусов. Целостность системы должна регулярно проверяться.

Требования к передаче:

1. Эта информация должна находиться внутри учреждения. Если её передача будет осуществляться по открытым каналам (например, интернет), то информация должна быть зашифрована.

2. Внутренняя информация не должна передаваться за пределы учреждении за исключением ситуаций из пункта 1.

Требования к уничтожению: отсутствуют.

18.4. Класс 3. Конфиденциальная информация.

Описание:

Данные этого класса конфиденциальны внутри учреждении и защищены от доступа извне. В случае доступа к этим данным посторонних возникает риск воздействия на эффективность учреждения, привести к ощутимым финансовым потерям, раскрытию данных о заказчиках и ином ущербе. Целостность данных жизненно важна. Примеры: размер заработной платы, персональные данные, бухгалтерская информация, данные о заказчиках, проектах и контрактах. Центры обработки данных обычно поддерживают этот уровень безопасности.

Требования к хранению:

1. ИТ системы, восприимчивые к вирусным атакам должна регулярно сканироваться на предмет обнаружения вирусов. Целостность системы должна регулярно проверяться. Настройка ИТ систем не должна допускать неавторизованную модификацию данных и программ.

2. Информация должна находиться в закрытых помещениях (например, документы и цифровые носители в закрываемых шкафах, компьютеры в закрываемых комнатах).

Требования к передаче:

1. Пароли не должны передаваться открытым текстом (ни в электронном, ни в печатном видах).

2. Эта информация должна находиться внутри учреждении. Если её передача будет осуществляться по открытым каналам (например, интернет), то информация должна быть зашифрована. Алгоритмы шифрования должны быть стойкими).

Требования к уничтожению:

1. Информация, которая больше не используется, должна быть надёжно уничтожена (документы в шредере, дискеты физически уничтожены).

18.5. Класс 4: Секретная информация.

Описание:

Неавторизованный доступ к этим данным извне или изнутри является критичным для учреждения. Целостность данных жизненно важна. Число лиц, имеющих доступ к этим данным должно быть минимальным. Следует

придерживаться очень строгих правил при использовании этих данных. Примеры: военная тайна, информация о планируемых крупных контрактах/реорганизации/финансовых операциях.

Требования к хранению:

1. ИТ системы, восприимчивые к вирусным атакам должна регулярно сканироваться на предмет обнаружения вирусов. Целостность системы должна регулярно проверяться. Настройка ИТ систем не должна допускать неавторизованную модификацию данных и программ и должна ежегодно подвергаться аудиту.

2. Информация должна находиться в закрытых помещениях (например, документы в закрываемых шкафах, компьютеры в закрываемых комнатах).

3. Информация должна храниться в зашифрованном виде или на съёмных носителях, физический доступ к которым ограничен.

Требования к передаче:

1. Пароли не должны передаваться открытым текстом (ни в электронном, ни в печатном видах).

2. Эта информация должна шифроваться во время передачи за пределы защищённых зон. Алгоритмы шифрования должны быть стойкими).

Требования к уничтожению:

1. Информация, которая больше не используется, должна быть надёжно уничтожена (документы в шредере, дискеты физически уничтожены).

19. Соблюдение законодательства и данной политики

19.1. Местные, национальные и международные правовые нормы (например, неприкосновенность данных, запрет на распространение порнографии) должны одинаково соблюдаться.

19.2. Интернет-порнография: интернет в настоящее время рассматривается как основной носитель незаконных материалов, от мягкой порнографии до педофилии и пропаганды нацизма.

Если подобный материал проходит через шлюз учреждении, он должен быть блокирован.

Персоналу не разрешается использовать компьютеры и другое оборудование учреждении для доступа к подобным материалам. Пользователи могут быть подвержены взысканию, если это распоряжение будет нарушено.

19.3. Законы о неприкосновенности личной жизни: персональные данные должны защищаться в соответствие с законами неприкосновенности личной жизни той страны, где они хранятся или обрабатываются.

20. Заключение

20.1. Настоящая Политика является внутренним документом Учреждения, общедоступной и подлежит размещению на официальном сайте Учреждения.

20.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики. Действующая редакция всегда находится на странице по адресу: https://ge74.ru.

20.3. Ответственность должностных лиц Учреждения, имеющих доступ к конфиденциальной информации, за невыполнение требований норм, регулирующих обработку и защиту информации, определяется в соответствии с законодательством Российской Федерации и внутренними документами Учреждения.

ГОСЭКСПЕРТИЗА
Челябинской области

Приложение 1
к Политике информационной безопасности
ОГАУ «Госэкспертиза Челябинской области»

Лист ознакомления
с Политикой информационной безопасности

№ п/п	ФИО работника	Дата ознакомления	Подпись работника
1	Аксенова Татьяна Евсеевна		
2	Антошкин Владимир Анатольевич		
3	Баева Татьяна Николаевна		
4	Белов Александр Вячеславович		
5	Белоусов Михаил Александрович		
6	Бондарь Людмила Лианфильдовна		
7	Булакова Евгения Вадимовна		
8	Ветюгов Иван Владимирович		
9	Видовский Юрий Корнеевич		
10	Волкова Ольга Викторовна		
11	Гаврилов Александр Сергеевич		
12	Головина Галина Ивановна		
13	Гордеева Лада Васильевна		
14	Громов Денис Анатольевич		
15	Исаев Антон Владимирович		
16	Кажура Лариса Васильевна		
17	Карякин Владислав Анатольевич		
18	Карякина Марина Петровна		
19	Копиняк Иван Михайлович		
20	Кошелева Елена Анатольевна		

21	Кулаев Иван Александрович		
22	Лаврова Елена Владимировна		
23	Майорова Наталья Викторовна		
24	Мартынова Анастасия Алексеевна		
25	Митусов Александр Владимирович		
26	Москвитина Елена Кирилловна		
27	Нагорная Анастасия Николаевна		
28	Некерова Татьяна Сабировна		
29	Никитина Наталья Сергеевна		
30	Носков Игорь Николаевич		
31	Палишкина Татьяна Владиславовна		
32	Подкорытова Ольга Генриховна		
33	Радионова Ольга Викторовна		
34	Растихина Ольга Викторовна		
35	Рудакова Илона Николаевна		
36	Сабельников Александр Николаевич		
37	Сафина Марина Вагизовна		
38	Севостьянова Анастасия Владимировна		
39	Старостина Людмила Васильевна		
40	Титова Екатерина Николаевна		
41	Урванцева Евгения Сергеевна		
42	Фенченко Дмитрий Валерьевич		
43	Языкова Ольга Викторовна		