Муниципальное казенное учреждение
Центр социальной помощи семье и детям

ПРИКАЗ

29.12.2018 № 639

Об утверждении Политики информационной безопасности

В соответствии с требованиями законодательства об информации, информационных технологиях и о защите информации, о защите персональных данных,

п р и к а з ы в а ю:

1. Утвердить Политику информационной безопасности муниципального казенного учреждения Центр социальной помощи семье и детям (Приложение 1 к настоящему приказу).

2. Заместителям директора, главному бухгалтеру обеспечить:

2.1. обеспечить ознакомление подчиненных работников с Политикой информационной безопасности;

2.2. осуществлять контроль над соблюдением подчиненными работниками положений Политики.

3. Контроль над исполнением настоящего приказа возложить на заместителя директора Такленок А.В.

Директор Н.Е. Демина

Приложение
к приказу от 29.12.2018 г.
№ 639

Политика информационной безопасности муниципального казенного учреждения Центр социальной помощи семье и детям

1. Введение

Политика информационной безопасности (далее – Политика) муниципального казенного учреждения Центр социальной помощи семье и детям (далее по тексту – Учреждение) определяет систему взглядов на проблему обеспечения информационной (далее – ИБ), и представляет собой систематизированное изложение высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы управления информационной безопасностью (далее – СУИБ) Учреждения.

Обеспечение информационной безопасности – необходимое условие для успешного осуществления уставной деятельности Учреждения.

Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Учреждение.

Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических и организационных мероприятий.

2. Обозначения и сокращения

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ИБ	Информационная безопасность
ИР	Информационный ресурс
ИС	Информационная система
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ОКЗ	Орган криптографической защиты
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СУИБ	Система управления информационной безопасностью

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

Конфиденциальность информации – состояние защищенности информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Несанкционированный доступ – доступ к информации иди действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обработка риска – процесс выбора и реализации мер по модификации (снижению) риска.

Политика – общие цели и указания, формально выраженные руководством.

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

Риск – сочетание вероятности события и его последствий.

Система управления информационной безопасностью (СУИБ) – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами.

События информационной безопасности – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

Угроза – опасность, предполагающая возможность потерь (ущерба).

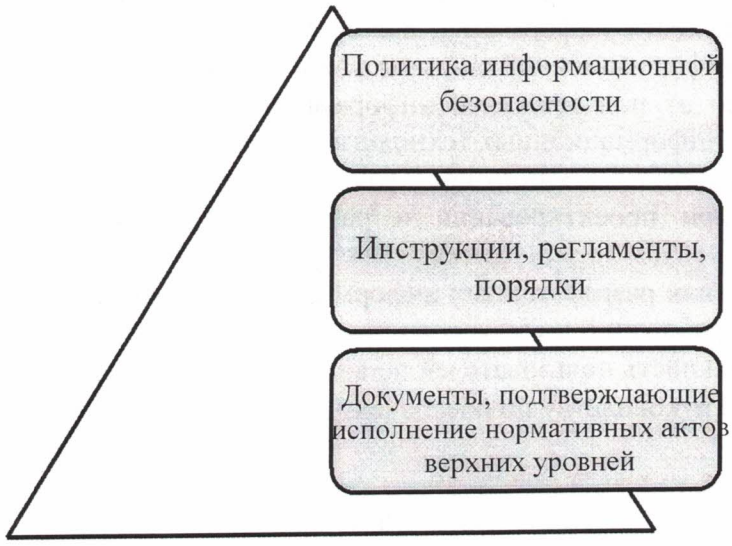
Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

4. Цель разработки Политики

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация рисков ИБ.

Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- соответствие требованиям Федерального законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
- обеспечение непрерывности критических процессов;
- достижение адекватности мер по защите от угроз ИБ;
- изучение партнеров, контрагентов и кандидатов на работу;
- недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;



Настоящая Политика является внутренним нормативным документом по ИБ **первого уровня**.

Документы **второго уровня** – инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников Учреждения по реализации документов первого и второго уровня.

Документы **третьего уровня** – отчетные документы о выполнении требований документов верхних уровней.

7.1.2. Ответственность за обеспечение ИБ

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Учреждении функции обеспечения ИБ возложены организационно-методическое отделение.

На это структурное подразделение возлагается решение следующих задач:

- проведение в жизнь Политики ИБ;
- определение требований к защите информации;
- организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты;
- оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;
- регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;
- обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях процессов;
- информирование, обучение и повышение квалификации работников Учреждения в сфере информационной безопасности;
- расследование инцидентов информационной безопасности
- сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности;
- обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений.

Для решения задач, возложенных организационно-методическое отделение, его сотрудники имеют следующие права:

учреждения. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков.

Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков.

Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

- учесть изменения требований и приоритетов;
- принять во внимание новые угрозы и уязвимости;
- убедиться в том, что реализованные средства сохранили свою эффективность.

Перед обработкой каждого риска Учреждение должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для Учреждения.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

- применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска, если он точно удовлетворяет Политике Учреждения и критериям принятия рисков;
- уклонение от риска путем недопущения действий, могущих быть его причиной;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

7.4. Безопасность персонала

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные соответствии с настоящей Политикой должны быть доведены до сотрудника при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как общие обязанности по реализации и поддержке политики безопасности, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

7.4.1. Условия приема на работу

Все принимаемые на работу сотрудники должны одобрить и подписать свои трудовые договоры, в которых устанавливается их ответственность за ИБ. В договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Учреждения по проверке выполнения требований ИБ, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения сотрудником требований ИБ.

Обязанности по обеспечению ИБ должны быть включены в должностные инструкции каждого сотрудника Учреждения.

Все принимаемые сотрудники должны быть ознакомлены под роспись с перечнем информации, ограниченного доступа, с установленным режимом с ней и с мерами ответственности за нарушение этого режима.

При предоставлении сотруднику доступа к ИС Учреждения он должен ознакомиться под роспись с инструкцией пользователя ИС.

7.4.2. Ответственность руководства

Руководство Учреждения должно требовать от всех сотрудников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в Учреждении политиками и процедурами.

Уполномоченные руководством Учреждения сотрудники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- выполнения действующих инструкций по вопросам ИБ;

7.5.5. Перемещение имущества

Оборудование, информация или ПО должны перемещаться за пределы Учреждения только при наличии письменного разрешения руководства. Сотрудники, имеющие право перемещать оборудование и носители информации за пределы Учреждения должны быть четко определены. Время перемещения оборудования за пределы Учреждения и время его возврата должны регистрироваться.

7.6. Контроль доступа

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.

Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламенту предоставления доступа пользователям.

Каждому пользователю, допущенному к работе с конкретным информационным активом Учреждения, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать с ИА.

В случае производственной необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных 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 учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

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

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

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

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

1) использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершенными ей действиями;

2) использование групповых ID разрешать только в случае, если это необходимо для выполнения задачи;

7.6.2. 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.).

7.6.3. 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 учетных записей, неактивных более 45 дней;
- включение учетных записей, используемых поставщиками для удаленной поддержки, только на время выполнения работ;

- выбрать фразу, которую легко запомнить. Например, «Три мудреца в одном тазу пустились по морю в грозу»;

- выбрать первые буквы из каждого слова «тмвотппмвг»;

- набрать полученную последовательность, переключившись на английскую раскладку клавиатуры: «nvdjnggvdu»;

- выбрать номер символа, который будет записываться в верхнем регистре и после которого будет специальный символ. Например, это будет пятый символ, а в качестве специального символа выбран «#». Получаем: «nvdjN#ggvdu».

Сотруднику запрещено:

- 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. Покидая рабочее место, пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

Сотрудник обязан:

1) в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации сотруднику организационно-методического отделения;

2) немедленно сообщить сотруднику организационно-методического отделения в случае получения от кого-либо просьбы сообщить пароль;

3) менять пароль каждые 90 дней;

4) менять пароль по требованию администратора ИБ.

После 20 неудачных попыток ввода пароля учетная запись блокируется на 10 минут. При систематической блокировке учетной записи работником (более 3 раз) оповещается Администратор ИБ.

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.

7.6.5. 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.

7.6.6. 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, защищенный 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 утвержден.

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

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ. Указанные работы, а так же работы по установке, регистрации и активации приобретенного лицензионного ПО могут быть выполнены только сотрудниками организационно-методического отделения.

Сведения о вновь приобретенном программном обеспечении должны быть внесены в перечень разрешенного программного обеспечения.

7.7.2. 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 организационно-методическое отделение.

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 закрепленных за ними АРМ, в определенное 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, определенный в стандарте рабочих мест Учреждения. Изменение установленной конфигурации возможно после внесения соответствующих поправок в стандарт рабочих мест или по служебной записке, согласованной с организационно-методическим отделением. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется организационно-методическим отделением.

Самостоятельная установка программного обеспечения на АРМ запрещена. Установка и удаление любого программного обеспечения производится только сотрудниками организационно-методического отделения.

В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в организационно-методическое отделение.

Сотрудники организационно-методического отделения 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 организационно-методическое отделение о любых фактах нарушения требований ИБ;
- ставить в известность организационно-методическое отделение о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;
- выполнять предписания организационно-методического отделения Учреждения;
- 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 организационно-методическое отделение.

При использовании ИС Учреждения запрещено:

• 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.

7.7.5. 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 разрешенного 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 приема и отправки документов с помощью электронной почты занимается делопроизводитель. Обеспечением порядка работы электронной почты в Учреждении занимается специалист организационно-методического отделения.

В Учреждении используется два адреса электронной почты:

beregn@bk.ru - предназначен для служебного использования всеми сотрудниками Учреждения для отправки и получения документов в электронном виде, служебной переписки; указывается на штампе Учреждения на бланке исходящего документа;

beregn-ok@mail.ru - предназначен для служебного использования только делопроизводителем, отвечающим за организацию документооборота в Учреждении; используется для отправки в структурные подразделения документов, расписанных директором к исполнению, и ответов на них в электронном виде, а также получения документов от иных органов социальной защиты.

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

Пользователям 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 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 дает согласие на ознакомление и иное использование в интересах Учреждения его переписки, осуществляемой с использованием электронной почты Учреждения, и

С уважением, <Фамилия имя>

<Номера телефонов, мессенджеры, адреса электронной почты>

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

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

7.7.6. Работа в сети

Доступ к информационно-телекоммуникационной сети «Интернет» предоставляется сотрудникам Учреждения в целях выполнения ими своих должностных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

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

При использовании сети Интернет необходимо:

- соблюдать требования настоящей Политики;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность организационно-методическое отделение 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;

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 пользователям к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

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.

7.7.7. Защита от вредоносного ПО

Организационно-методическое отделение регулярно проверяет сетевые ресурсы Учреждения антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

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, надежности 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.

7.8.3.1. Требований по обеспечению ИБ при использовании СКЗИ

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 утвержденные стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

7.8.3.2. 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.

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

7.8.4. Безопасность системных файлов

Чтобы свести к минимуму риск повреждения ИС, в учреждении необходимо обеспечить контроль над внедрением ПО в рабочих системах.

Тестовые данные должны находиться под контролем и защитой. Для испытаний обычно требуются значительные объемы тестовых данных, максимально близко соответствующие рабочим данным. Необходимо избегать использования рабочих баз данных, содержащих конфиденциальную информацию. Если эти базы все же будут использоваться, то конфиденциальные данные должны быть удалены или изменены.

7.8.5. Безопасность процесса разработки и обслуживания систем

Чтобы свести к минимуму вероятность повреждения ИС Учреждения, следует ввести строгий контроль над внесением изменений. Необходимо установить официальные правила внесения изменений. Эти правила должны гарантировать, что процедуры, связанные с безопасностью и контролем, не будут нарушены, что программисты, занимающиеся поддержкой, получат доступ только к тем частям системы, которые необходимы для их работы, и что для выполнения любого изменения требуется получить официальное разрешение и подтверждение.

После внесения изменений в ИС критичные для процессов Учреждения приложения должны анализироваться и тестироваться, чтобы гарантировать отсутствие вредных последствий для безопасности Учреждения.

Следует препятствовать внесению изменений в пакеты ПО, за исключением необходимых изменений. Все изменения должны строго контролироваться.

7.9. Управление инцидентами информационной безопасности

В Учреждении должна быть разработана и утверждена формальная процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

Все сотрудники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях.

В дополнение к уведомлению о происшествиях ИБ и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов ИБ.

Цели управления инцидентами ИБ должны быть согласованы с руководством для учета приоритетов Учреждения при обращении с инцидентами.

Необходимо создать механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

7.10. Управление непрерывностью и восстановлением

Необходимо разработать контролируемый процесс для обеспечения и поддержки непрерывности процессов Учреждения. Данный процесс должен объединять в себе основные элементы поддержки непрерывности процессов.

В Учреждении должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности

- 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 надежности и безопасности ИС;

- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

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

7.13. Предоставление услуг сторонним организациям

7.13.1. Соглашения о предоставлении услуг

В соглашения о предоставлении услуг сторонним организациям должны быть включены требования безопасности, описание, объемы и характеристики качества предоставляемых услуг.

7.13.2. Анализ предоставления услуг

Услуги, отчеты и записи, предоставляемые сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

- контроль объема 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 отчетов о предоставленных услугах;
- управление любыми обнаруженными проблемами.

8. Ответственность

Директор Учреждения определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ Учреждения.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Учреждения лежит на руководстве организационно-методического отделения.

Все руководители несут прямую ответственность за реализацию Политики и ее соблюдение персоналом в соответствующих подразделениях.

Работники Учреждения несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в организационно-методическое отделение.

В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей.

Руководство Учреждения регулярно проводит совещания, посвященные проблемам обеспечения информационной безопасности с целью формирования четких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.