ДЕПАРТАМЕНТ КУЛЬТУРЫ
ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА - ЮГРЫ

БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА - ЮГРЫ «МУЗЕЙ ГЕОЛОГИИ, НЕФТИ И ГАЗА»

ПРИКАЗ

«02» июля 2024 года № 132/2-ОД

«Об утверждении Политики информационной безопасности бюджетного учреждения Ханты-Мансийского автономного округа - Югры «Музей геологии, нефти и газа»

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», п р и к а з ы в а ю :

1. Утвердить Политику информационной безопасности бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Музей геологии, нефти и газа» (далее – Политика) (Приложение №1 к настоящему приказу).
2. Начальнику отдела информационных технологий Магрычеву А.А. не позднее 3-х рабочих дней, с момента подписания настоящего приказа разместить Политику на официальном сайте бюджетного учреждения Ханты-Мансийского автономного округа - Югры «Музей геологии, нефти и газа».
3. Документоведу отдела правовой, организационной и кадровой работы, в установленном порядке ознакомить под подпись с настоящим приказом руководителей структурных подразделений.
4. Приказ вступает в силу с момента его подписания.
5. Контроль за исполнением настоящего приказа возложить на заместителя директора по развитию А.Ю. Салыкину.

Директор А.В. Паньков

Приложение №1
к Приказу БУ «Музей геологии, нефти и газа»
от «02» июля 2025 г. №132/2-ОД

УТВЕРЖДАЮ
Директор бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Музей геологии, нефти и газа»

_____А.В. Паньков
М.П.

Политика информационной безопасности бюджетного учреждения Ханты-Мансийского автономного округа - Югры «Музей геологии, нефти и газа»

1. Общее содержание

1.1. Политика информационной безопасности бюджетного учреждения Ханты-Мансийского автономного округа – Югры Музей геологии, нефти и газа (далее – Политика, Учреждение) определяет систему взглядов на проблему обеспечения информационной безопасности (далее - ИБ). 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.

1.2. 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.

1.3. Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищённости 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.

1.4. **Обозначения и сокращения**

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БУ	Бюджетное учреждение
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

1.5. **Термины и определения**

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

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

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

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

Документ - зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

Доступность информации - состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

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

Идентификация - присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

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

Информационная безопасность (ИБ) - состояние защищённости интересов Учреждения.

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

Информационный процесс - процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационный ресурс - всё, что имеет ценность и находится в распоряжении Учреждения.

Инцидент - непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Инцидент информационной безопасности - одно или серия нежелательных, или неожиданных событий ИБ, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу ИБ.

Контролируемая зона - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

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 защищённости информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

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

Политика - общие цели и указания, формально выраженные руководством.

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

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

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 неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

2. Цели и задачи

2.1. Основной целью является обеспечение информационной безопасности Учреждения, что предполагает эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности, подчиненное единому замыслу.

2.2. Главная цель принимаемых мер защиты информации Учреждения состоит в том, чтобы гарантировать целостность, достоверность, доступность и конфиденциальность информации во всех ее видах и формах, включая документы и данные, обрабатываемые, хранимые и передаваемые в информационно-вычислительных и телекоммуникационных системах (далее - информационные системы) Учреждения независимо от типа носителя этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности Учреждения, не жертвуя при этом основными принципами информационной безопасности, описанными в данной Политике. Ответственность за организацию и проведение работ по обеспечению информационной безопасности несет начальник отдела информационных технологий.

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

2.4. 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;

– недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;

– выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников.

3. Область действия

3.1. Настоящая Политика распространяется на все структурные подразделения Учреждения и обязательна для исполнения всеми его сотрудниками и должностными лицами.

3.2. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах.

3.3. Настоящая политика распространяется на информационные системы Учреждения.

3.4. Лица, осуществляющие разработку внутренних документов Учреждения, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

4. Содержание политики

4.1. Система управления информационной безопасностью

Для достижения указанных целей и задач в Учреждении внедряется система управления информационной безопасностью.

СУИБ документирована в настоящей политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех работников Учреждения в области действия системы. Документированные требования СУИБ доводятся до сведения работников Учреждения.

4.1.1. Структура документов

В целях создания взаимосвязанной структуры нормативных документов Учреждения в области обеспечения информационной безопасности, разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:

– Политика информационной безопасности является внутренним нормативным документом по ИБ **первого уровня;**

– Инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников Учреждения по реализации документов первого и второго уровня — это документы **второго уровня**

– Отчётные документы о выполнении требований документов верхних уровней это документы **третьего уровня.**

4.1.2. Ответственность за обеспечение ИБ

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Учреждении функции обеспечения ИБ возложены на отдел информационных технологий (далее – отдел ИТ).

На это подразделение возлагается решение следующих основных задач:

– 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;

– расследования инцидентов информационной безопасности;

– сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности;

Для решения задач, возложенных на отдел ИТ, его сотрудники имеют следующие права:

– определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области;

– получать информацию от пользователей информационных систем Учреждения по любым аспектам применения информационных технологий в Учреждении;

– участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;

– участвовать в испытаниях, разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;

– контролировать деятельность пользователей по вопросам обеспечения ИБ;

– готовить предложения руководству по обеспечению требований ИБ.

4.2. Объект защиты

Объектом защиты в контексте данной Политики являются информационные ресурсы Учреждения обрабатываемые в информационных системах и ее функциональных подсистемах, содержащие сведения, доступ к которым ограничен, и используемые в процессах сбора, обработки, накопления, хранения и распространения в границах информационных систем.

Основными объектами защиты в Учреждении являются:

– информационные ресурсы Учреждения ограниченного распространения, в том числе содержащие конфиденциальные сведения;

– программные информационные ресурсы Учреждения, а именно: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

– физические информационные ресурсы Учреждения: компьютерное аппаратное обеспечение всех видов;

– носители информации всех видов (электронные, бумажные и прочие);

– все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением.

Следует также отметить, что указанные выше основные объекты защиты являются наиболее ценными ресурсами, и, следовательно, по отношению к ним должны применяться самые эффективные правила и методы защиты. И доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения имиджа Учреждения, эффективности его функционирования и т.д.

Доступность, целостность и конфиденциальность в обязательном порядке должны учитываться при разработке организационно-распорядительной документации по обеспечению информационной безопасности для системы в целом и для каждого ее ресурса в отдельности.

4.3. Оценка рисков

Для оценки рисков при составлении и последующем пересмотре организационно-распорядительных документов необходимо систематически рассматривать следующие аспекты:

–ущерб, который может нанести деятельности Учреждения серьезное нарушение информационной безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации;

- реальную вероятность такого нарушения защиты в свете превалирующих угроз и средств контроля.

4.4. Безопасность персонала

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с Политикой ИБ Учреждения, 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.

4.4.1. Условия найма

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.

4.4.2. 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;
- данных, находящихся на носителях информации;
- порядка использования сотрудниками информационных ресурсов;
- содержания служебной переписки.

4.4.3. Обучение ИБ

Все сотрудники должны проходить периодический инструктаж в области политики и процедур ИБ, принятых в Учреждении.

Основной целью обучения является:

- обеспечение уверенности в осведомленности сотрудников Учреждения об угрозах и проблемах, связанных с информационной безопасностью, об ответственности в соответствии с законодательством;
- знание работниками правильного использования средств обработки информации прежде, чем им будет предоставлен доступ к информации или услугам;
- оснащение работников Учреждения всем необходимым для соблюдения требований политики безопасности при выполнении служебных обязанностей.

Работники Учреждения должны знать и выполнять требования организационно-распорядительных документов (в части касающейся) Учреждения в области информационной безопасности, требования обеспечения безопасности обработки информации на средствах вычислительной техники, правила работы в сети Интернет.

Работники Учреждения должны уметь работать с операционными системами MS Windows, семейства UNIX на уровне пользователя, антивирусным программным

обеспечением, офисным программным обеспечением, средством архивации (7-Zip) должны уметь пользоваться встроенной справкой.

4.4.4. Завершение или изменения трудовых отношений

При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

4.5. Физическая безопасность

4.5.1. Защищённые области

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Учреждения, должны быть размещены в защищенных областях. Такими средствами являются: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации.

Защищённые области должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающими возможность доступа только авторизованного персонала.

Запрещается приём посетителей в помещениях, когда осуществляется обработка информации ограниченного доступа.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, металлическими шкафами или шкафами, оборудованными замком. Помещения должны быть обеспечены средствами уничтожения документов.

4.5.2. Области общего доступа

Места доступа, через которые неавторизованные лица могут попасть в помещения Учреждения, должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа.

4.5.3. Вспомогательные службы

Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС Учреждения.

4.5.4. Утилизация или повторное использование оборудования

Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все конфиденциальные данные и лицензионное ПО. Отсутствие защищаемой информации на носителях должно быть проверено специалистами отдела информационных технологий, о чём должна быть сделана отметка в акте списания.

4.5.5. 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 чётко определены. Время перемещения оборудования за пределы Учреждения и время его возврата должны регистрироваться.

4.5.6. Правила физической защиты

4.5.6.1. Перед внедрением и использованием нового аппаратного, программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо разработать для него правила обеспечения безопасности и использовать их наряду с правилами, изложенными в данном разделе.

4.5.6.2. Перед установкой и использованием какого-либо компьютерного аппаратного обеспечения в обязательном порядке следует ознакомиться с информацией, предоставленной разработчиком (продавцом), и строго ей следовать.

4.5.6.3. Перед проведением крупной модернизации или ремонта, перед выполнением манипуляций непосредственно с носителями информации необходимо выполнить резервное копирование данных.

4.5.6.4. После выполнения процесса модернизации аппаратного и (или) программного обеспечения необходимо обязательно провести внеплановое техническое обслуживание всей системы.

4.5.6.5. При размещении компьютерного оборудования в помещении, а также в процессе его эксплуатации приоритетным является обеспечение для его безопасного функционирования, соответствующего положениям, изложенным в прилагаемой к нему документации. В период простоя устройства необходимо обеспечить сохранность его работоспособности и внешнего вида.

4.5.6.6. Всю документацию на компьютерное оборудование и программное обеспечение (гарантийные обязательства производителей (продавцов), руководства пользователей (User's Manual), регистрационные карточки, кассовые и товарные чеки и прочее) должны обязательно сохраняться после покупки и храниться в надежном, защищенном от света и других вредоносных воздействий месте в упаковке.

4.5.6.7. Следует в полном объеме и неукоснительно соблюдать правила эксплуатации тех или иных аппаратных компьютерных компонентов.

4.5.6.8. Техническое обслуживание компьютерного оборудования и программного обеспечения (физическая чистка оборудования, поддержание программного обеспечения в работоспособном состоянии и т.д.) следует производить регулярно, желательно в соответствии с заранее составленным расписанием и с учетом рекомендаций разработчиков данного оборудования и программ (с данными рекомендациями следует внимательно ознакомиться до выполнения каких-либо действий по обслуживанию).

4.5.6.8.1. Техническим обслуживанием считаются также и мероприятия по резервному копированию данных, которые должны неукоснительно исполняться. Они должны выполняться строго регулярно и не реже, чем раз в неделю. Если это возможно, стоит сделать повторную копию данных и размещать ее на хранение отдельно от первой. Сразу же после проведения резервного копирования данных необходимо каким-либо способом убедиться в работоспособности и корректности полученной копии.

4.5.6.8.2. Резервному копированию в обязательном порядке подлежат:

- все конфиденциальные данные сотрудников в автоматизированной системе;
- любые другие данные согласно решению уполномоченных работников Учреждения.

4.5.6.8.3. Во время резервного копирования данных, а также во время записи любой информации на носители информации однократной записи, нельзя производить другие виды работ на той компьютерной системе, при помощи которой осуществляется эта запись.

4.5.6.8.4. Все носители (электронные, бумажные и др.) с конфиденциальной информацией и резервными копиями этой и другой информации должны храниться в недоступном для посторонних, защищенном от света и других вредоносных воздействий месте с соблюдением правил безопасного хранения для данного вида носителя информации. Носителям с особо ценной информацией следует уделять повышенное внимание.

4.5.6.8.5. Все расходные материалы следует использовать максимально эффективно, не допуская нерационального их использования. Все расходные материалы (используемые в данный момент и неиспользуемые) необходимо хранить в строгом соответствии с правилами их хранения.

4.5.6.8.6. Желательно предпринять ряд мер по энергосбережению для тех устройств, которые временно не используются или находятся в состоянии ожидания.

4.5.6.8.7. Запрещается курить, употреблять пищу и напитки непосредственно вблизи компьютера. Необходимо предпринять меры, чтобы обезопасить компьютерное оборудование от повреждения в данном случае.

4.5.6.8.8. В течение внедрения и использования нового аппаратного, программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо приложить все усилия к тому, чтобы научиться эффективно его применять.

4.5.6.8.9. Необходимо в обязательном порядке записать все наиболее важные установки и настройки системы в состоянии ее нормального (штатного) функционирования.

Подобные записи приравниваются к аппаратной (программной) документации и должны соответствующим образом обслуживаться.

4.5.6.8.10. Необходимо размещать системы вывода информации (мониторы, дисплеи и т.д.) компьютеров так, чтобы они не были видны со стороны двери, окон и тех мест в помещениях, которые не контролируются.

4.5.6.8.11. Необходимо предпринять ряд мер, благодаря которым компьютерные системы пользователя будут обеспечены стабильным электропитанием. Обязательным является использование хотя бы самых простых средств по обеспечению надежности электропитания системы (сетевые фильтры, заземление и т.д.).

4.5.6.8.12. При возникновении какой-либо аварийной ситуации необходимо немедленно прекратить эксплуатацию аварийного устройства. Немедленно поставить в известность начальника отдела информационных технологий.

Соответствующему отделу информационных технологий в кратчайшие сроки организовать мероприятия по его ремонту или замене.

4.5.6.8.13. Следует составить подробные технологические схемы для проведения различного рода мероприятий, связанных с аппаратным и программным обеспечением (техническое обслуживание, правила техники безопасности, резервное копирование данных и т.п.).

4.5.6.8.14. Необходимо рассмотреть возможность применения различных систем автоматизированного мониторинга текущего состояния аппаратных информационных ресурсов, и при первой же возможности внедрить их, по крайней мере, на наиболее важных и ответственных участках.

4.5.6.8.15. В течение процесса списания компьютерной техники, носителей информации и др. необходимо позаботиться о том, чтобы после выполнения процедуры переноса основных информационных ресурсов со списываемой техники, было произведено полное и безвозвратное уничтожение содержащейся на ней конфиденциальной и любой другой информации.

4.5.6.8.16. Необходимо обязательно разработать план действий по продолжению работы и обеспечению безопасности данных на случай, если выйдут из строя какие-либо аппаратные и (или) программные части компьютерной системы. Данный план должен систематически проверяться на актуальность и при необходимости пересматриваться.

4.6. Контроль доступа

Основными пользователями информации в информационной системе Учреждения являются сотрудники Учреждения. 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.

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

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

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы.

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

использование одной общей пользовательской учётной записи разными пользователями запрещено.

Регистрируемые учётные записи подразделяются на:

– пользовательские - предназначенные для аутентификации пользователей ИР Учреждения;

– системные - используемые для нужд операционной системы;

– служебные - предназначенные для функционирования отдельных процессов или приложений.

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

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

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

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

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

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

– предоставление и блокирование прав должны быть санкционированы и документированы;

– уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;

– документальная фиксация назначенных пользователю прав доступа;

– ознакомление пользователей под подпись с письменными документами, в которых регламентируются их права доступа;

– предоставление доступа с момента завершения процедуры регистрации;

– обеспечение создания и поддержания формального списка всех пользователей, зарегистрированных для работы с ИР или сервисом;

– немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из Учреждения;

– аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;

– обеспечение того, чтобы лишние ID пользователей не были доступны другим пользователям.

4.6.1. 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;

– 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;

– пароль должен состоять не менее чем из шести символов, состоять из произвольных комбинаций букв, цифр и других символов или же представлять собой бессмысленную комбинацию слов, включающую буквы верхнего регистра;

– необходимо изменять пароля пользователя не реже одного раза в полгода.

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.).

4.6.2. Использование паролей

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

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

4.6.2.3. Значение пароля учетной записи пользователя устанавливает Администратор информационной безопасности ИСПДн.

4.6.2.4. Личные пароли устанавливаются сотрудниками отдела информационных технологий. Пароли устанавливаются пользователям автоматизированной системы с учетом следующих требований:

– длина пароля должна быть не менее 6-ти буквенно-цифровых символов;

– в числе символов пароля должны присутствовать три из четырёх видов символов:

1. буквы в верхнем регистре;

2. буквы в нижнем регистре;

3. цифры;

4. специальные символы (! @ # $ % л & * ( ) - _ + - ~ [ ] { } j \ : ; < > , . ? /);

– пароль не должен содержать легко вычисляемые сочетания символов, например, 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;

– при смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях;

- для различных ИС необходимо устанавливать собственные, отличающиеся пароли.

4.6.2.5. Сотруднику запрещается:

– сообщать свой пароль кому-либо;

– указывать пароль в сообщениях электронной почты;

– хранить пароли, записанные на бумаге, в легко доступном месте;

– использовать тот же самый пароль, что и для других систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.);

– использовать один и тот же пароль для доступа к различным корпоративным ИС.

4.6.2.6. Сотрудник обязан:

– в случае подозрения на то, что пароль стал кому-либо известен, обратиться к специалисту отдела информационных технологий и сообщить о факте компрометации;

– немедленно сообщить специалисту отдела информационных технологий в случае получения от кого-либо просьбы сообщить пароль;

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

4.6.2.8. 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.

4.6.3. Пользовательское оборудование, оставляемое без присмотра

4.6.3.1. Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра.

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

4.6.4. Политика чистого стола

4.6.4.1. 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;

- завершении сеанса выходить из системы у универсальных ЭВМ, серверов и офисных ПК.

4.6.4.2. Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утверждён.

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

4.6.4.4. Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра.

4.6.4.5. 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»),

4.6.4.6. Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.

4.6.4.7. В конце рабочего дня сотрудник должен привести в порядок письменный стол и убрать все офисные документы в запираемый шкаф или сейф.

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

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

4.7. Политика допустимого использования информационных ресурсов

Общие обязанности пользователя:

- при работе с ПО руководствоваться нормативной документацией (руководством пользователя);

- обращаться в службу поддержки пользователей или к специалистам, назначенными ответственными за системное администрирование и информационную безопасность, по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), а также за необходимой методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;

- знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;

- минимизировать вывод на печать обрабатываемой информации.

Пользователю запрещено производить несанкционированное

распространение справочной информации, которая становится доступна при подключении к корпоративной ИС Учреждения.

4.7.1. Использование ПО

В Учреждении допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения.

Запрещено незаконное хранение на жестких дисках Учреждения информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

Решение о приобретении и установке программного обеспечения, необходимого для реализации финансовых, административно-хозяйственных и других задач принимает начальник отдела информационных технологий.

Документы, подтверждающие покупку программного обеспечения, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся в отделе ИКТ,

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ. Указанные работы, а также работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только сотрудниками отдела информационных технологий.

Сведения о вновь приобретённом программном обеспечении должны быть внесены в перечень разрешённого программного обеспечения.

4.7.2. Использование АРМ и ИС

К работе в ИС Учреждения допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.

4.7.3. Политика допустимого использования информационных ресурсов

Каждому сотруднику Учреждения, которому необходим доступ к ИР в рамках его должностных обязанностей, выдаются под роспись необходимые средства автоматизации. Ответственность по установке и поддержке всех компьютерных систем, функционирующих в Учреждении, возложена на отдел ИТ.

Все АРМ, установленные в Учреждении, имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией, определённый в стандарте рабочих мест Учреждения. Изменение установленной конфигурации возможно после внесения соответствующих поправок в стандарт рабочих мест или по служебной записке, согласованной с отделом ИТ. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется отделом ИТ.

Самостоятельная установка программного обеспечения на АРМ запрещена.

Установка и удаление любого программного обеспечения производится только сотрудниками отдела ИТ.

В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в отдел ИТ.

Сотрудники отдела ИТ 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:

1. знать и выполнять требования внутренних организационно- распорядительных документов Учреждения;

2. использовать ИС и АРМ Учреждения исключительно для выполнения своих служебных обязанностей;

3. ставить в известность отдел ИТ о любых фактах нарушения требований ИБ;

4. ставить в известность отдел ИТ о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;

5. незамедлительно выполнять предписания отдела ИТ Учреждения.

6. при необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;

7. в случае необходимости продолжения работы по окончании рабочего дня проинформировать об этом отдел ИТ.

При использовании ИС Учреждения запрещено:

1. использовать АРМ и ИС в личных целях;

2. отключать средства управления и средства защиты, установленные на рабочей станции;

3. передавать:

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

Информация о посещаемых ресурсах ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Учреждения.

Все электронные сообщения и документы в электронном виде, передаваемые посредством ИС Учреждения, подлежат обязательной проверке на отсутствие вредоносного ПО.

4.7.4. Использование ресурсов локальной сети

Для выполнения своих служебных обязанностей сотрудники обеспечиваются доступом к соответствующим информационным ресурсам.

Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Учреждения, базы данных, электронная почта.

Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы. Временное расширение прав доступа осуществляется отделом ИТ

Учреждения в соответствии с Порядком предоставления (изменения) полномочий пользователя.

4.7.5. Обработка конфиденциальной информации

При обработке конфиденциальной информации сотрудники обязаны:

- знать и выполнять требования Инструкции по работе с конфиденциальной информацией;

- при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети Учреждения применять средства защиты от неавторизованного доступа;

- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;

- не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;

- обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;

- не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;

- не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;

- не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD - диски, Flash - устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

4.7.6. Использование электронной почты

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

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

При работе с электронной почтой Учреждения пользователь должен учитывать:

– электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;

– электронная почта не является средством передачи информации, гарантирующим конфиденциальность передаваемой информации (передачу конфиденциальной информации вне локальной сети Учреждения необходимо осуществлять только в зашифрованном виде);

– электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

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

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

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

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

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

Использование корпоративной электронной почты Учреждения для частной переписки сотрудником, надлежащим образом, ознакомленным с данной Политикой, является нарушением трудовой дисциплины Учреждения. Подписываясь в ознакомлении с настоящей Политикой, сотрудник даёт согласие на ознакомление и иное использование в интересах Учреждения его переписки, осуществляемой с использованием корпоративной электронной

почты, и соглашается с тем, что любое использование его переписки, осуществляемой с использованием корпоративной электронной почты, не может рассматриваться как нарушение тайны связи.

Каждый сотрудник Учреждения имеет право на просмотр либо иное использование в интересах Учреждения сообщений корпоративной электронной почты, которые направлены или получены им, соответственно, с его или на его корпоративный электронный адрес.

Использование сообщений корпоративной электронной почты осуществляется уполномоченными сотрудниками Учреждения в соответствии с их функциями, определёнными в данной Политике и в иных локальных нормативных актах Учреждения. Просмотр и иное использование сообщений электронной почты в интересах Учреждения осуществляется сотрудниками Учреждения в целях обеспечения защиты конфиденциальных сведений, обеспечения нормальной работоспособности системы электронной почты, в рамках обслуживания сервисов электронной почты, при выполнении ручной пересылки сообщений, приходящих на корпоративные электронные адреса Учреждения сотрудникам или группам сотрудников, а также по мотивированным запросам прямых или непосредственных руководителей любых сотрудников, чью почту необходимо использовать в интересах Учреждения.

Использование сообщений корпоративной электронной почты в интересах Учреждения, в том числе ознакомление с содержанием сообщений, осуществляется в соответствии с правами доступа к информации, установленными внутренними Положениями о конфиденциальной информации и иными правовыми актами, регламентирующими порядок обращения с информацией ограниченного доступа.

Исходящие электронные сообщения сотрудников Учреждения должны содержать следующие поля:

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

Формат подписи отправителя:

С уважением,
< Фамилия имя>
<Должность>
<Структурное подразделение> <Наименование Учреждения> <Адрес>
<номера контактов: телефон, мессенджеры, адреса электронной почты> <сайт>

Формат предупреждения о служебном характере сообщения и его конфиденциальности:

«Это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию. Настоящим уведомляем Вас о том, что, если это сообщение не предназначено Вам, использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых действий на основе этой информации, строго запрещено и защищается законодательством Российской Федерации. Если Вы получили это сообщение по ошибке, пожалуйста, сообщите об этом отправителю по электронной почте и удалите это сообщение. CONFIDENTIALITY NOTICE: This email and any files attached to it are confidential. If you are not the intended recipient you are notified that using, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited and protected by the laws of the Russian Federation. If you have received this email in error please notify the sender and delete this email. »

При формировании ответов на полученные электронные сообщения можно использовать следующую упрощённую подпись:

С уважением,

<Фамилия имя>

<Номера телефонов, мессенджеры, адреса электронной почты>

В случае получения служебного сообщения о невозможности доставки сообщения адресату или получения извещения от адресата о том, что он не получил отправленное ему сообщение, необходимо связаться с сотрудником отдела ИТ.

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.

4.7.7. Работа в сети

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

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

При использовании сети Интернет необходимо:

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

Использовании сети Интернет запрещено:

1. использовать предоставленный Учреждением доступ в сеть Интернет в личных целях;
2. использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
3. совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Учреждения;
4. публиковать, загружать и распространять материалы, содержащие:

- конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с отделом ИТ;
- угрожающую, клеветническую, непристойную информацию;
- вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;
- фальсифицировать свой IP- адрес, а также прочую служебную информацию.

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

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

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

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

4.7.8. Защита от вредоносного ПО

Отдел ИТ регулярно проверяет сетевые ресурсы Учреждения антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник Учреждения должен незамедлительно оповестить об этом отдел ИТ. После чего администратор ИБ должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

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

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

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;
- периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте.

4.8. Приобретение, разработка и обслуживание систем

4.8.1. Требования безопасности для информационных систем

При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности.

Требования к безопасности и средства защиты должны соответствовать ценности используемых ИР и потенциальному ущербу для Учреждения в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками.

Системные требования к ИБ и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования ИС.

4.8.2. Корректная обработка информации

Данные, вводимые в прикладные системы, необходимо проверять, чтобы гарантировать их правильность и соответствие поставленной задаче.

4.8.3. Криптографические средства

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

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

Для конфиденциальной 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.

4.8.3.1. Требований по обеспечению ИБ при использовании СКЗИ

Шифрование — это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной 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 12В бит.

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

4.8.3.2. 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. Вынос электронной цифровой подписи (ЭЦП) за пределы служебного помещения запрещён, поскольку это может привести к нарушению производственной деятельности организации. Несанкционированное использование ЭЦП вне стен учреждения повышает вероятность утечки конфиденциальной информации, что способно вызвать сбои в работе автоматизированных процессов, снижение эффективности взаимодействия между подразделениями и задержку исполнения поручений руководства. Для предотвращения негативных последствий, сохранность ЭЦП должна обеспечиваться исключительно в пределах контролируемого офисного пространства.

Дополнительно к общему ограничению на вынос электронной цифровой подписи (ЭЦП) за пределы служебного помещения, сотрудники обязаны заблаговременно подавать руководителю подразделения и начальнику отдела информационных технологий либо его замещающему лицу письменное заявление на предоставление временной копии ЭЦП. Заявление должно содержать обоснование необходимости выдачи разрешения и сопровождаться согласием на контроль за использованием выданной копии. Выдача дубликата ЭЦП возможно лишь после согласования с соответствующими должностными лицами в письменной форме и оформления специального распоряжения, которое обеспечивает строгий контроль за использованием копии и предотвращает возможные утечки конфиденциальной информации и угрозы информационной безопасности в организации.

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.

4.8.3.3. Управление ключами

Управление криптографическими ключами важно для эффективного использования криптографических средств.

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

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

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

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

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

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

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

Необходимо обеспечивать защиту открытых ключей от угроз подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей.

Сертификаты необходимо изготавливать таким способом, который однозначно связывал бы информацию, относящуюся к владельцу пары открытого/секретного ключей, с открытым ключом. Поэтому важно, чтобы процессу управления, в рамках которого формируются эти сертификаты, можно было доверять.

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

4.8.4. 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 объёмы тестовых данных, максимально близко соответствующие рабочим данным. Необходимо избегать использования рабочих баз данных, содержащих конфиденциальную информацию. Если эти базы всё же будут использоваться, то конфиденциальные данные должны быть удалены или изменены.

4.8.5. 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.

4.9. 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 учёта приоритетов Учреждения при обращении с инцидентами.

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

4.10. Управление непрерывностью и восстановлением

Основной целью управления непрерывностью работы Учреждения является противодействие прерывания работы и защита рабочих процессов от последствий при значительных сбоях или бедствиях.

Необходимо обеспечивать управление непрерывностью работы с целью минимизации отрицательных последствий, вызванных нарушениями безопасности. Последствия от нарушений безопасности и отказов в обслуживании необходимо анализировать, по результатам анализа разрабатывать и внедрять планы обеспечения непрерывности работы с целью восстановления рабочих процессов в течение требуемого времени при их нарушении. Такие планы следует поддерживать и применять на практике. Должна быть выработана стратегия непрерывности рабочего процесса в соответствии с согласованными целями и приоритетами. Необходимо, чтобы планирование непрерывности работы начиналось с идентификации событий, которые могут быть причиной прерывания работы, например отказ оборудования, наводнение или пожар. Планирование должно сопровождаться оценкой рисков с целью определения последствий этих прерываний (как с точки зрения масштаба

повреждения, так и периода восстановления). Оценка риска должна распространяться на все рабочие процессы и не ограничиваться только средствами обработки информации. В зависимости от результатов оценки рисков необходимо разработать стратегию для определения общего подхода к обеспечению непрерывности работы. Разработанный план должен быть утвержден руководством Учреждения. Необходимо, чтобы план обеспечения непрерывности работы предусматривал следующие мероприятия по обеспечению информационной безопасности:

– определение и согласование всех обязанностей должностных лиц и процедур на случай чрезвычайных ситуаций;

– внедрение в случае чрезвычайных ситуаций процедур, обеспечивающих возможность восстановления рабочего процесса в течение требуемого времени;

– особое влияние следует уделять оценке зависимости работы от внешних факторов и существующих контрактов;

– документирование согласованных процедур и процессов;

– соответствующее обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление.

Необходимо, чтобы план обеспечения непрерывности работы соответствовал требуемым целям работы.

4.11. Соблюдение требований законодательства

Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Учреждения к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, достоверности и конфиденциальности ИР, содержащих персональные данные, начиная от стадии сбора и ввода данных до их хранения. Персональные данные конкретного сотрудника и процесс их обработки должен быть открытым для этого сотрудника.

В Учреждении должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного ПО.

Важная документация Учреждения должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства, подзаконных актов, контрактных обязательств и требований.

Система хранения и обработки должна обеспечивать чёткую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Эта система должна иметь возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются Учреждению.

Криптографические средства должны использоваться в соответствии со всеми имеющимися соглашениями, законодательными и нормативными актами.

4.12. Аудит информационной безопасности

Учреждение должно проводить своими силами внутренние проверки СУИБ через запланированные интервалы времени. 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.

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.

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

5. Ответственность

5.1. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Учреждения лежит на начальнике отдела информационных технологий.

5.2. Начальник отдела информационных технологий 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.

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

5.4. Работники Учреждения несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в отдел ИТ.

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

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

5.7. Нарушение требований нормативных актов Учреждения по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

5.8. Ответственность за выполнение правил Политики ИБ несет каждый сотрудник Учреждения в рамках своих должностных обязанностей и полномочий.

5.9. На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования Политики ИБ Учреждения, могут быть подвергнуты дисциплинарным взысканиям.

5.10. Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Учреждению в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Учреждения несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

6. Контроль и пересмотр Политики

6.1. Общий контроль состояния ИБ Учреждения осуществляется начальником отдела информационных технологий.

6.2. Текущий контроль соблюдения настоящей Политики осуществляет отдел информационных технологий. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Учреждения, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

6.3. Отдел информационных технологий ежегодно пересматривает положения настоящей политики. Изменения и дополнения вносятся по инициативе начальника отдела информационных технологий и утверждаются директором Учреждения.