УТВЕРЖДАЮ
Директор СПб ГБУ
"ДК "Парголовский"
Э.И.Аксенова
"01" марта 2023 г.
Приложение № 1
к приказу от 01.03.2023 № 17

Политика информационной безопасности Санкт-Петербургского государственного бюджетного учреждения "Дом культуры "Парголовский"

2023 год

Оглавление

Определения

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами.

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

Конфиденциальность – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким – либо признакам.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Обозначения и сокращения

ДК – Дом культуры;

КИ – Конфиденциальная информация

МЭ – Межсетевой экран

НДС – Несанкционированный доступ

СЗИ – Система защиты информации

СКЗИ – Средство криптографической защиты информации

СрЗИ – Средство защиты информации

ФСБ России – Федеральная служба безопасности Российской Федерации

ФСТЭК России – Федеральная служба по техническому и экспортному контролю

1. Общие положения

1.1. Настоящее Политика является документом, доступным всем сотрудникам ДК и всем пользователям его ресурсов. Представляет собой официально принятую руководством ДК систему взглядов на обеспечение информационной безопасности в ДК.

1.2. Основной задачей в области информационной безопасности ДК признает совершенствование мер и средств обеспечения информационной безопасности информационных ресурсов ДК в контексте развития законодательства и норм регулирования информационной деятельности.

1.3. В рамках своей деятельности ДК обязуется предпринимать все возможные меры для защиты информации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности и других противоправных действий, связанных с нарушением информационной безопасности ДК.

1.4. Требования информационной безопасности, которые предъявляются ДК, соответствуют целям деятельности ДК и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.5. Реализация и контроль исполнения требований, установленных настоящей Политикой, осуществляется работниками ДК, ответственных за информационную безопасность, в соответствии со всеми должностными инструкциями и другими внутренними документами ДК по информационной безопасности.

2. Цели и задачи обеспечения информационной безопасности

2.1. Целями обеспечения информационной безопасности ДК являются:

- защита интересов ДК, работников и иных субъектов информационных отношений, взаимодействующих с ДК, от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем ДК, нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;

- обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов ДК и предоставляемых сервисов;

- соблюдение правового режима использования массивов и программ обработки информации;

- предотвращение реализации угроз для деятельности ДК.

2.2. Объектами информационных правоотношений являются:

- информационные ресурсы, в том числе с ограниченным доступом;

- процессы обработки информации в информационных системах ДК, информационные технологии, регламенты сбора обработки, хранения и передачи информации;

- информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства с ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации;

- системы и средства защиты информации, объекты и помещения, в которых размещены хранилища информации.

2.3. Субъектами информационных отношений при использовании информационных систем ДК, заинтересованными в обеспечении информационной безопасности, являются:

- ДК, как собственник информационных ресурсов и оператор персональных данных;

- работники подразделений ДК, как пользователи и поставщики информации в информационные системы;

- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах ДК.

2.4. Субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности определенной части информации;

- целостности информации;

- своевременного доступа к необходимой им информации;

- защиты от навязывания им ложной (недостоверной, искаженной) информации;

- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных отношений и установленных правил обращения с информацией;

- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

-защиты соответствующей части информации от незаконного ее тиражирования и распространения.

2.5. Для достижения целей защиты и обеспечения указанных свойств информации, система обеспечения информационной безопасности ДК должна обеспечивать решение следующих задач:

- Защиту от вмешательства в процессе функционирования информационных систем посторонних лиц (возможность использования системы и доступ к ее ресурсам должны иметь только зарегистрированные пользователи).

- Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационных систем (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей).

- Регистрацию и периодический контроль действий пользователей при использовании защищаемых ресурсов и периодический контроль корректности их действий.

- Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения.

- Защиту от несанкционированной модификации и контроль целостности используемых в ДК программных средств и данных, а также защиту от несанкционированного внедрения вредоносных программ.

- Защиту информации ограниченного доступа, хранимой, обрабатываемой в ДК, от несанкционированного разглашения или искажения.

- Обеспечение ДК аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации), а также определение автора при создании и модификации информации.

- Обеспечение исправности применяемых в информационных системах ДК средств защиты информации.

- Своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации.

- Создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации в ДК.

2.6. Решение вышеперечисленных задач в ДК осуществляется:

- Учетом всех подлежащих защите информационных ресурсов (каналов связи, аппаратных и программных средств).

- Регламентацией процессов обработки подлежащей защите информации, действий работников ДК и персонала, осуществляющего обслуживание и модификацию программных и технических средств, на основе утвержденных организационно- распорядительных документов по вопросам обеспечения информационной безопасности.

- Назначением и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в ДК.

- Наделением каждого работника минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам.

- Знанием и строгим соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

- Персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам информационных систем.

- Реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения технических средств и данных.

- Принятием мер по обеспечению физической целостности технических средств информационных систем и поддерживанием необходимого уровня защищенности их компонентов.

- Использованием физических и технических (программно-аппаратных) средств защиты ресурсов ДК и административной поддержкой их использования.

- Контролем соблюдения пользователями информационных систем требований по обеспечению информационной безопасности.

- Юридической защитой интересов ДК при взаимодействии с юридическими и физическими лицами от противоправных и несанкционированных действий со стороны этих лиц.

- Проведением анализа эффективности принятых мер и применяемых средств защиты информации в ДК. Разработкой и реализацией предложений по совершенствованию СЗИ в ДК.

3. Принципы обеспечения информационной безопасности

3.1. Принцип законности

- При выборе защитных мероприятий, реализуемых системой обеспечения информационной безопасности, должно соблюдаться действующее законодательство.

- Принятые меры защиты не должны препятствовать доступу к защищаемой информации со стороны государственных или правоохранительных органов, если такой доступ необходим в случаях, предусмотренных законодательством.

- Программно-технические средства, применяемые в ДК, должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств.

3.2.Принцип системности

При построении системы обеспечения информационной безопасности необходимо применять системный подход, который предполагает взаимосвязь процессов организации защиты информационных ресурсов ДК, согласованное применение методов и средств защиты информационных ресурсов ДК.

3.3. Принцип координации

- При организации действий по обеспечению информационной безопасности руководство ДК обеспечивает четкую взаимосвязь соответствующих структурных подразделений между собой, с представителями сторонних организаций, оказывающих услуги в рамках договорных обязательств.

- При построении, внедрении и эксплуатации системы обеспечения информационной безопасности руководство ДК обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

3.4. Принцип дружественности и простоты

- Система обеспечения информационной безопасности в ДК формируется таким образом, чтобы сделать максимально прозрачными для пользователей информационных систем ДК процессы ее функционирования.

- Система обеспечения информационной безопасности в ДК выстраивается таким образом, чтобы ограничения организованного и технического характера, налагаемые на сотрудников ДК в связи с реализацией защитных мер, существенно не затрудняли работу с ресурсами информационных систем ДК.

3.5. Принцип превентивности

Меры, применяемые ДК с целью обеспечения информационной безопасности, должны носить упреждающий характер и не допускать реализацию соответствующих угроз и атак.

3.6. Принцип оптимальности и многоуровневости

- Выбор единых программно-технических средств с целью сокращения расходов на создание и поддержку функционирования компонентов системы обеспечения информационной безопасности.

- Применение разнородных программно-технических средств защиты, с целью построения целостной системы обеспечения информационной безопасности и устранения возможных уязвимостей.

- Использование для создания разных рубежей обеспечения информационной безопасности средств, которые имеют схожие друг с другом функции, но разработанные различными производителями и имеющие различную логику построения защитных механизмов.

3.7. Принцип экономической целесообразности

- Осуществление оценки уровня затрат на обеспечение безопасности, ценности информационных ресурсов и величины возможного ущерба для ДК в случае нарушения конфиденциальности, целостности и доступности информационных ресурсов.

- Выбор необходимого и достаточного уровня защиты информационных ресурсов, при котором затраты, риск и размер возможного ущерба являются приемлемыми.

3.8. Принцип непрерывности и недопустимости открытого состояния

- Система обеспечения информационной безопасности в ДК строится таким образом, чтобы процесс защиты информационных систем ДК осуществлялся непрерывно на протяжении всего жизненного цикла информационных систем.

- Система обеспечения информационной безопасности в ДК при любых возникающих обстоятельствах либо полностью выполняет свои функции, либо полностью блокирует доступ.

3.9. Принцип профессионализма

- Привлечение для разработки и внедрения систем обеспечения информационной безопасности, при необходимости, специализированных организаций, наиболее подготовленных к конкретному виду деятельности и имеющих соответствующие лицензии на выполнение работ и практический опыт в данной области.

- Организация профессиональной подготовки своих работников для эксплуатации обеспечения информационной безопасности.

3.10. Принцип выбора решений защиты

- Ориентация на применение современных высокотехнологичных решений и программно-технических средств защиты, хорошо зарекомендовавших себя, интуитивно понятых и не сложных в эксплуатации.

- Использование оценки степени корректности функционирования и исполнения защитных функций, отказоустойчивости, проверки согласованности конфигурации различных компонентов и возможности осуществления централизованного администрирования при выборе решений по защите информационных систем.

3.11. Принцип развития

- Развитие и обновление на регулярной основе существующей системы обеспечения информационной безопасности.

- Ориентация на преемственность принятых ранее решений по защите, на анализ функционирования информационных систем и самой системы обеспечения информационной безопасности.

3.12. Принцип персональной ответственности и разделение обязанностей

- Руководство ДК определяет права и ответственность каждого конкретного работника (в пределах его должностных обязанностей) за обеспечение информационных ресурсов ДК.

- Система обеспечения информационной безопасности ДК обеспечивает разделение полномочий в информационных системах, обязанностей и ответственности между работниками, исключающее возможность нарушения критически важных для ДК процессов и создания уязвимостей в защите информационных ресурсов.

3.13. Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих функций в ДК, в соответствии со своими должностными обязанностями.

4. Зоны ответственности участников процесса обеспечения информационной безопасности.

4.1. Руководство ДК

- Создает условия, при которых каждый работник знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликтов интересов.

- Назначает работников, ответственных за создание и использование СЗИ, информации обрабатываемой в ДК, реализацию процессов обеспечения информационной безопасности, а также их контроля.

- Обеспечивает достаточную численность и квалификацию персонала, ответственного за построение и поддержание процессов обеспечения информационной безопасности, внедрение и управление СЗИ, а также контроль и мониторинг текущего состояния системы обеспечения информационной безопасности.

- Инициирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в ДК.

- Анализирует результаты работ обеспечения информационной безопасности и на их основе принимает решения о необходимости развития системы обеспечения информационной безопасности, ее развития, о возможности принятия остаточных рисков информационной безопасности, о выделении ресурсов, необходимых для реализации Политики информационной безопасности.

4.2. Компетентные подразделения ДК

- Подготавливают предложения по доработке Политики информационной безопасности в части технического обеспечения информационных систем ДК.

- Разрабатывают процедуры эффективного управления техническими и программными средствами информационных систем и применяют их в практической деятельности в отношении всех систем, действующих в ДК.

- Обеспечивают защиту доступа ко всему серверному и коммутационному оборудованию, носителям информации, которые используются в соответствующих структурных подразделениях.

- Осуществляют мероприятия по поддержке сопровождения и использования информационных систем.

- Обеспечивают отказоустойчивость всего программно-аппаратного комплекса и процедуру регламентированного восстановления работоспособности после отказов компонентов.

- Регулярно обновляют программные и программно-аппаратные комплексы СЗИ в ДК.

- Осуществляют поддержку функционирования информационных систем и принимают необходимые меры по конфигурированию систем обеспечения необходимого уровня информационной безопасности.

- Контролируют работоспособность устройств бесперебойного питания критичных для ДК информационных систем.

- Обеспечивают физическую защиту помещений, в которых располагаются критичные для ДК информационные системы.

- Обеспечивают сопровождение устройств контроля доступа в помещения.

- Обеспечивают защиту информационных ресурсов ДК от случайного или намеренного уничтожения, искажения, разглашения.

- Контролируют выполнение установленных правил и процедур обеспечения информационной безопасности.

4.3. Руководители структурных подразделений

- Обязаны соблюдать требования действующего законодательства российской Федерации и внутренних документов ДК в части обеспечения информационной безопасности.

- Обеспечивают контроль за соблюдением норм и правил обеспечения информационной безопасности в своем структурном подразделении и информируют компетентное подразделение о любых подозрительных событиях или нарушениях действующих правил обеспечения информационной безопасности.

- Обеспечивают соответствие действий работников подразделения Политике информационной безопасности, внутренним документам по информационной безопасности и любым другим распоряжениям руководства ДК по вопросам информационной безопасности.

- Организуют проведение необходимого инструктажа по вопросам выполнения правил информационной безопасности для всех работников структурного подразделения.

- Контролируют выполнение работниками в своем структурном подразделении установленных правил в целях обеспечения физической безопасности компьютерного оборудования и носителей информации.

- Своевременно информируют руководство о всех выявленных сбоях в работе информационных систем.

- Контролируют доступ к необходимым информационным ресурсам работников своего структурного подразделения в соответствии с потребностью в пределах служебных обязанностей.

4.4. Работники ДК

- Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов, документов ДК по вопросам информационной безопасности.

- Соблюдают конфиденциальность данных, доступ к которым был ими получен.

- Обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе.

- Не допускают самовольного и использования в автоматизированной информационной системе личного компьютерного и цифрового оборудования, а также носителей информации.

- Не допускают самовольную установку программного обеспечения на компьютеры, входящие в состав информационной системы.

- Своевременно информируют руководителя своего структурного подразделения о всех случаях нарушения информационной безопасности и о всех выявленных сбоях в работе программных и программно- аппаратных средств.

- Проявляют осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.

4.5. Сторонние физические и юридические лица

- Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов ДК и других распоряжений руководства по вопросам информационной безопасности при исполнении договорных обязательств.

5. Основные требования по защите информации ограниченного доступа

5.1. Общие требования

- В ДК необходимо соблюдать режим безопасности, предусматривающий реализацию организационно-технических мероприятий, направленных на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с требованиями законодательства Российской Федерации.

- В ДК осуществляется обработка и хранение информации ограниченного доступа (доступ к которой ограничен федеральными законами и служебной необходимостью).

- В ДК должен быть разработан перечень информации ограниченного доступа.

- ДК, как обладатель информации ограниченного доступа, при осуществлении своих прав обязано:

а) соблюдать права и законные интересы иных лиц;

б) принимать меры по защите информации;

в) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

- ДК, как обладатель информации ограниченного доступа, если иное не предусмотрено федеральными законами, вправе:

а) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

б) использовать информацию, в том числе распространять ее, по своему усмотрению;

в) передавать информацию другим лицам на установленном законом основании;

г) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

д) осуществлять иные действия с информацией или разрешать осуществление таких действий, если эти действия не противоречат федеральным законам и другим нормативно-правовым актам регуляторов.

- ДК, являясь обладателем информации ограниченного доступа, в случаях, установленных законодательством Российской Федерации, обязано обеспечивать:

а) предотвращение НСД к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

б) своевременное обнаружение фактов НСД к информации;

в) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

г) возможность регламентированного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

д) постоянный контроль за обеспечением уровня защищенности информации.

- Защита информации ограниченного доступа представляет собой принятие правовых, организационных и технических мер, направленных на:

а) соблюдение конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);

б) обеспечение целостности информации (исключение неправомерного уничтожения или модифицирования информации);

в) реализацию права на доступ к информации (исключение неправомерного блокирования информации).

5.2. Организация защиты конфиденциальной информации

- При организации в ДК защиты информации ограниченного доступа, необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации.

- В ДК необходимо соблюдать режим защиты конфиденциальной информации (далее –КИ):

а) ограничение доступа к КИ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

б) учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;

в) регулирование отношений по использованию КИ, с работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

г) использование материальных носителей, содержащих КИ в соответствии с утвержденным порядком, исключающим доступ к ним.

- Для обеспечения защиты КИ, ДК вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству РФ, меры.

- В целях охраны КИ, в рамках трудовых отношений необходимо:

а) ознакомить под расписку работников, доступ которых к КИ, необходим для выполнения ими служебных обязанностей, с перечнем КИ, и установленным в ДК режимом защиты КИ, а также мерами ответственности за его нарушение;

б) создать работникам необходимые условия для соблюдения установленного режима защиты КИ.

- Работники ДК, обязаны выполнять установленный в ДК режим защиты КИ, не разглашать информацию, составляющую КИ, и не использовать эту информацию в личных целях.

5.3 Особенности защиты персональных данных

- При организации в ДК защиты персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», которые регулируют отношения, связанные с обработкой и хранением персональных данных граждан и определяет требования по защите их конфиденциальности.

- ДК самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом № 152-ФЗ или другими федеральными законами.

- Перечень мер, выполнение которых обеспечивает ДК в качестве оператора персональных данных, должен включать:

а) назначение в ДК ответственного за организацию обработки персональных данных;

б) издание ДК документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

в) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ;

г) оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона 152-ФЗ, соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом №152-ФЗ;

д) ознакомление работников ДК, непосредственно осуществляющих обработку персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ДК в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и обучение, при необходимости, указанных работников.

- ДК при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, копирования, предоставления, распространение персональных данных.

- Обеспечение безопасности персональных данных достигается в частности:

а) определение угроз и нарушителей безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн);

б) проведение классификации ИСПДн в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», и определение класса защищенности для ИСПДн;

в) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает выбранные уровни защищенности персональных данных;

г) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

д) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

е) учетом машинных носителей персональных данных;

ж) обнаружением фактов НСД к персональным данным и принятием мер;

з) восстановлением персональных данных, модифицированных или уничтоженных вследствие НСД к ним;

и) установлением правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;

к) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн.

- Работники ДК должны быть ознакомлены под роспись с документами ДК, устанавливающими порядок обработки персональных данных, а также об их правах, обязанностях и ответственности.

6. Основные требования к процессам обеспечения информационной безопасности

6.1. Общие положения

Методическое руководство, разработку конкретных требований по защите информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации осуществляют компетентные подразделения ДК.

6.2. Физическая безопасность и безопасность на рабочем месте

- Система защиты зданий и помещений ДК, объектов и технических средств информационных систем ДК обеспечивает выполнение следующих функций:

а) разграничение доступа работников в помещения ДК в соответствии с их полномочиями и функциональными обязанностями;

б) регистрацию фактов входа посторонних лиц в здание ДК;

в) предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;

г) разрешительный режим вноса/выноса (ввоза/вывоза) компьютерного оборудования, средств записи и хранения информации.

- Определяется перечень технических средств, находящихся в специальных контролируемых зонах.

- К техническим средствам, которые выделяются в специальные контролируемые зоны необходимо отнести следующие группы ресурсов:

а) Основные информационные серверы и средства вычислительной техники, на которых осуществляется обработка и хранение информации ограниченного распространения;

б) сетевое оборудование и серверы, обеспечивающие работу критических систем;

в) файловые серверы, на которых хранятся данные, в том числе резервные;

г) критичные для деятельности ДК системы и коммуникационное оборудование, обеспечивающее внешние коммуникации ДК.

- Контролируемые зоны защищаются соответствующими системами контроля и управления доступом, обеспечивая доступ только авторизованному персоналу.

- Доступ в контролируемые зоны сторонних лиц или представителей других организаций возможен только в сопровождении уполномоченного работника ДК.

- Размещение и эксплуатация рабочих станций, серверов и сетевого оборудования осуществляется в помещениях, оборудованных замками, средствами сигнализации и (при необходимости) постоянно находящихся под охраной или наблюдением.

- Размещение технических средств вывода и отображения информации в помещениях ДК производится с учетом исключения возможности визуального просмотра информации посторонними лицами и персоналом, не допущенным к работе с данной информацией.

- Работники ДК на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей с защищаемой информацией.

- Технические средства и оборудование должны размещаться и храниться таким образом, чтобы сократить возможный риск его повреждения и угрозы несанкционированного доступа.

- Помещения ДК должны быть оборудованы детекторами огня и дыма, огнетушителями, средствами охранно-пожарной сигнализации.

- Основное техническое оборудование ДК должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам ДК в соответствии с рекомендациями производителя.

- Пользователи портативных технических средств не должны оставлять техническое оборудование и носители без присмотра.

- Портативные технические средства не должны оставаться за пределами контролируемой зоны ДК дольше, чем того требует служебная необходимость, если иное не определено руководством ДК.

6.3. Безопасность при работе с носителями информации

- В ДК должны соблюдаться меры по безопасной работе с электронными носителями информации с целью контроля их использования, для предотвращения несанкционированного копирования и разглашения защищаемой информации, внесения изменений или уничтожения указанной информации, а также внесение изменений в работу информационных систем.

- Работники должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в ДК в иных целях строго запрещено.

- Электронные носители информации в ДК должны быть учтены путем присвоения каждому носителю инвентаризационного номера и назначения владельца.

- Электронные носители информации должны храниться в помещениях, исключающих получения к ним НСД, при этом должен быть обеспечен контроль доступа к носителям.

- Для контроля процессов использования и хранения электронных носителей информации должен быть разработан порядок плановой инвентаризации носителей.

- В случае кражи или потери электронных носителей информации, а также иных инцидентов, которые могут привести к разглашению защищаемой информации, должны проводиться мероприятия по расследованию указанных инцидентов.

- При снятии электронного носителя информации с эксплуатации, все данные, хранящиеся на нем, должны быть гарантированно стерты.

- При утилизации электронных носителей информации должна быть обеспечена невозможность восстановления записанной на них информации.

- Факт уничтожения информации и утилизации носителя информации фиксируется в соответствии с порядком, установленном в ДК.

6.4. Техническое обслуживание оборудования

- Технические средства всех систем ДК должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

- Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированным персоналом.

- Техническое обслуживание оборудования и систем сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации.

6.5. Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности ДК при взаимодействии с третьими лицами должны выполняться следующие мероприятия:

- заключение соглашения о неразглашении конфиденциальной информации;

- контроль за действиями третьих лиц;

- в договорах с третьими лицами предусматривать право ДК на проведение аудита обеспечения безопасности той информации, которая передается третьими лицам.

6.6. Управление жизненным циклом информационных систем

- Мероприятия по управлению жизненным циклом автоматизированных информационных систем должны быть направлены на обеспечение информационной безопасности при вводе в действие, эксплуатации, сопровождении и модернизации, вывода из эксплуатации информационных систем, автоматизирующих деятельность ДК.

- Основой при выборе или разработке информационных систем должны являться технические задания, содержащие требования информационной безопасности для информационных систем.

- Любое планируемое к внедрению изменение информационной системы предварительно должно быть протестировано на совместимость и отсутствие нарушений работоспособности системных компонентов.

- Работы по модернизации автоматизированной информационной системы, в том числе по установке программного обеспечения и обновлений, должны проводиться в нерабочее время или время наименьшей рабочей нагрузки.

- При выводе из эксплуатации автоматизированных информационных систем должно обеспечиваться гарантированное удаление обрабатываемой и хранимой в них информации с использованием специализированных программных средств или путем уничтожения носителей информации.

- Все процедуры обеспечения информационной безопасности, установленные в ДК в отношении информационных систем, должны выполняться и контролироваться ответственными за информационную безопасность лицами.

6.7. Антивирусная защита должны регулярно обновляться.

- В целях предупреждения, обнаружения и устранения вредоносных программ в ДК на постоянной основе должны использоваться средства антивирусной защиты.

- Обязательному антивирусному контролю должна подлежать любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация, хранимая на подключаемых съемных носителях, при непосредственном обращении к ней.

- При установке программного обеспечения на серверы информационных систем ДК или их обновлении должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

- Сигнатурные базы вредоносного программного обеспечения и антивирусные средства защиты должны регулярно обновляться.

- Пользователи информационных систем ДК не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

- В ДК необходимо определить процедуру для обработки и восстановления инфицированных данных и отслеживание источника заражения.

6.8. Контроль доступа к информационным системам

- Все работник ДК, допущенные к работе с информационными системами несут персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи в их распоряжении защищаемых ресурсов системы.

- Уровень полномочий пользователя в информационной системе ДК должен определяться в соответствии с его должностными обязанностями и производственной необходимостью.

- Доступ пользователей к информационным системам ДК должен контролироваться администратором системы.

- Осуществление регулярного контроля выполнения политик и иных документов, касающихся регламентации допуск работников к информационным системам.

6.9. Идентификация и аутентификация

- Доступ пользователей к информационным системам должен предоставляться только после успешного завершения процедур идентификации, аутентификации и авторизации.

- Получение пользователем имени в системе и парольной информации, которые обеспечивают доступ пользователя к ресурсам системы, должно осуществляться по представлению руководителей структурных подразделений.

6.10. Безопасность пароля

- С целью обеспечения защиты от несанкционированного доступа к информационным системам устанавливаются требования к выбору парольной информации, обеспечивающие достаточную степень стойкости паролей.

- Для обеспечения конфиденциальности парольной информации пользователю запрещается хранить значения своих паролей на бумажном носителе в открытом виде и в свободном доступе.

- Для обеспечения конфиденциальности парольной информации пользователям запрещается передавать значения своих паролей третьим лицам.

- При вводе пароля пользователем для доступа к информационной системе ДК должно исключаться отображение парольной информации на экране монитора в открытом виде.

- Процедура смены парольной информации в информационных системах ДК должна проводиться на регулярной основе.

6.11. Регистрация событий

Осуществление регистрации событий безопасности на всех компонентах информационных систем ДК, в которых обрабатывается, храниться или по средствам которых передается защищаемая информация.

6.12. Использование СКЗИ

- Решение об использовании СКЗИ в интересах защиты собственных информационных ресурсов принимается руководством ДК в соответствии с законодательством Российской Федерации.

- При эксплуатации СКЗИ и ключевой информации все сотрудники ДК должны выполнять требования нормативных правовых актов, издаваемых федеральным органом исполнительной власти в области обеспечения безопасности, документов ДК по обеспечению

безопасности использования СКЗИ, а также эксплуатационной документации производителя СКЗИ.

6.13. Безопасность информационной сети

- Установление надлежащего контроля в отношении локальной вычислительной сети и всех внешних информационных коммуникаций ДК для обеспечения защиты данных и защиты информационных систем ДК от НСД.

- Должны быть определены цели использования сети Интернет и требования к процедуре использования ресурсов сети Интернет. Использования сети Интернет работников в личных целях должно быть строго запрещено.

- Доступ к информационным сервисам сети Интернет предоставляется работникам ДК только в случае производственной необходимости.

- Подключение к сети Интернет должно осуществляться только при организации защиты соединения путем установки МЭ и специальных программных средств защиты.

- Разрешительные политики доступа в Интернет должны технически реализовываться специализированным программным обеспечением.

- Контроль использования работниками ресурсов сети Интернет должен осуществляться уполномоченными работниками на постоянной основе.

6.14. Использование корпоративной электронной почты

- Система корпоративной электронной почты должна использоваться в ДК с целью организации обмена электронными сообщениями между работниками, а также между работниками ДК и внешними абонентами.

- В ДК должны быть четко определены требования к использованию системы корпоративной электронной почты.

- Предоставление и прекращение доступа к ресурсам корпоративной электронной почты должно осуществляться только на основе оформленной заявки.

- В ДК должно быть установлено специальное программное обеспечение, осуществляющее контроль всех входящих сообщений на наличие вредоносного программного обеспечения.

- В ДК должны быть предусмотрены механизмы архивирования и резервного копирования корпоративной электронной почты в автоматическом режиме.

6.15. Резервное копирование и восстановление данных

- Осуществление резервного копирования для:

а) файловых серверов и серверов приложений, критичных для деятельности ДК;

б) операционных систем файловых серверов и прикладных программ;

в) приложений, критичных для деятельности ДК;

г) рабочих данных.

- Частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и допустимое время восстановления.

- Резервное копирование и восстановление ресурсов информационных систем ДК должны проводить уполномоченные работники ДК.

- Резервное копирование должно осуществляться в автоматическом режиме с применением специализированного программно-аппаратного комплекса.

7. Основные требования к процессам управления информационной безопасностью

7.1. Управление рисками

- Выбор требований по информационной безопасности и защитных механизмов, применяемых в системе информационной безопасности, должен основываться на проведении анализа рисков нарушения основных свойств безопасности для наиболее критичных информационных ресурсов ДК.

- Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения свойств целостности, конфиденциальности и доступности для ресурсов информационной системы ДК.

- Результатом проведения анализа рисков должен быть комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность ДК при реализации той или иной угрозы и обеспечивающих достаточный уровень защищенности информационных систем ДК.

7.2. Управление инцидентами информационной безопасности

- Для обеспечения эффективного разрешения инцидентов информационной безопасности в ДК, минимизации потерь и уменьшения риска возникновения повторных инцидентов должно осуществляться эффективное управление инцидентами информационной безопасности.

- Для управления инцидентами информационной безопасности должна быть создана система учета произошедших инцидентов, которая представляет собой комплекс средств мероприятий для сбора консолидации информации об инцидентах.

- В отношении каждого произошедшего инцидента должен выполняться его анализ и разработка эффективных мер реагирования на данный инцидент.

7.3. Мониторинг текущего уровня информационной безопасности

- Для обеспечения высокого уровня в отношении системы обеспечения информационной безопасности в ДК на постоянной основе должен проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности.

- Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов.

- При проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в ДК, уполномоченные работники должны придерживаться следующих принципов:

а) не нарушать функционирование текущей деятельности ДК;

б) действовать в соответствии с внутренними документами ДК по информационной безопасности;

в) не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;

г) оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности.

- Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к функционированию защитных мер, должна консолидироваться и храниться в местах, исключающих получения к ней несанкционированного доступа.

- Мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться, по возможности, с использованием встроенных механизмов настройки и аудита в программных и программно-технических средствах, используемых в информационных системах ДК.

7.4. Аудит системы обеспечения информационной безопасности

- В целях оценки текущего уровня информационной безопасности уполномоченные работники ДК на регулярной основе должны проводить аудит информационной безопасности.

- Внутренние аудиты или самооценки должны выполняться, по возможности, работниками ДК.

- Результатом выполнения аудитов по информационной безопасности должны стать отчеты о выполненном аудите информационной безопасности, которые разрабатываются специалистами ДК.

- По результатам аудита уполномоченные работники и ответственные подразделения ДК должны определить действия, необходимые для устранения обнаруженных несоответствий в процессе аудита и вызвавших их причин.

7.5. Управление персоналом

- Организация такого процесса управления персоналом, который обеспечит доверительное отношение к работникам, а также организует комплексное противодействие угрозам информационной безопасности, исходящим от персонала ДК.

- Выполнение обязательных проверок при приеме новых работников на работу с точки зрения достоверности сообщаемых ими данных и с позиции оценки их профессиональных навыков.

- Организация работы в направлении повышения осведомленности и обучения в области информационной безопасности.

- Повышение осведомленности работников ДК:

а) по существующим в ДК политикам информационной безопасности;

б) по применяемым в ДК защитным мерам;

в) по правильному использованию защитных мер в соответствии с внутренними документами ДК.

8. Заключение

- Настоящая Политика является внутренним документом администрации, общедоступной и подлежит размещению на официальном сайте ДК.

- Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики. Действующая редакция всегда находится на странице по адресу: https://dkpargolovo.1c-umi.ru.

- Контроль исполнения требований настоящей Политики осуществляется ответственным лицом за обеспечение безопасности персональных данных ДК

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