Приложение 10
к приказу МБОУ «Гимназия № 42»
от 29.12.2018 г. № 314-осн

ПОЛИТИКА
информационной безопасности МБОУ «Гимназия № 42»

1. Перечень используемых определений, обозначений и сокращений

АИБ – Администратор информационной безопасности.
АРМ – Автоматизированное рабочее место.
АС – Автоматизированная система.
ИБ – Информационная безопасность.
ИР – Информационные ресурсы.
ИС – Информационная система.
МЭ – Межсетевой экран.
НСД – Несанкционированный доступ.
ОС – Операционная система.
ПБ – Политики безопасности.
ПДн – Персональные данные.
ПО – Программное обеспечение.
СЗИ – Средство защиты информации.
ЭВМ – Электронная-вычислительная машина, персональный компьютер.

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

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Доступ к информации – возможность получения информации и ее использования.

Идентификация – присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – это актив, который, подобно другим активам общества, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и

т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений МБОУ «Гимназия № 42».

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационные ресурсы – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Источник угрозы – намерение или метод, нацеленный на умышленное использование уязвимости, либо ситуация или метод, которые могут случайно проявить уязвимость.

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

Конфиденциальность – доступ к информации только авторизованных пользователей.

Критичная информация – информация, нарушение доступности, целостности, либо конфиденциальности которой, может оказать негативное влияние на функционирование подразделений МБОУ "Гимназия №131" или иного вида ущерба.

Локальная вычислительная сеть – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

Межсетевой экран – программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав сети, а также между сетью МБОУ «Гимназия № 42» и внешними сетями (сетью Интернет).

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Политика информационной безопасности – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в МБОУ «Гимназия № 42» для обеспечения его информационной безопасности.

Пользователь локальной вычислительной сети – сотрудник организации (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в сети в установленном порядке и получивший права на доступ к ресурсам сети в соответствии со своими функциональными обязанностями.

Программное обеспечение – совокупность прикладных программ, установленных на сервере или ЭВМ.

Рабочая станция – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

Регистрационная (учетная) запись пользователя – включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п.

Роль – совокупность полномочий и привилегий на доступ к информационному ресурсу, необходимых для выполнения пользователем определенных функциональных обязанностей.

Ответственный за техническое обеспечение – сотрудник организации, занимающийся сопровождением автоматизированных систем, отвечающий за функционирование локальной сети МБОУ «Гимназия № 42» и ПК.

Угрозы информации – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т.е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Общества при реализации угроз в информационной сфере.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Вводные положения

Политика ИБ муниципального бюджетного общеобразовательного учреждения «Гимназия № 42» (далее – МБОУ «Гимназия № 42») определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется МБОУ «Гимназия № 42» в своей деятельности.

Основными целями политики ИБ являются защита информации МБОУ «Гимназия № 42» от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Уставе МБОУ «Гимназия № 42».

Общее руководство обеспечением ИБ осуществляется заместителем директора по УВР МБОУ «Гимназия № 42». Ответственность за организацию

мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет АИБ. Ответственность за функционирование информационных систем МБОУ «Гимназия № 42» несет администратор информационной системы.

Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.

Сотрудники МБОУ «Гимназия № 42» обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов внутренних документов МБОУ «Гимназия № 42» по вопросам обеспечения ИБ.

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

Наибольшими возможностями для нанесения ущерба МБОУ «Гимназия № 42» обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне МБОУ «Гимназия № 42»), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

Категории нарушителей и их возможности определяются в «Модели нарушителя».

На основе вероятностной оценки определяется перечень актуальных угроз безопасности, который отражается в «Модели угроз».

Для противодействия угрозам ИБ в МБОУ «Гимназия № 42» на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная СУИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для МБОУ «Гимназия № 42». Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Задачами настоящей политики являются:

– описание организации систему управления информационной безопасностью в МБОУ «Гимназия № 42»;

– определение Политик ИБ, а именно: политика реализации антивирусной защиты; политика учетных записей; политика предоставления доступа к ИР; политика использования паролей; политика защиты АРМ; политика конфиденциального делопроизводства;

– определение порядка сопровождения ИС МБОУ «Гимназия № 42».

Настоящая Политика распространяется на МБОУ «Гимназия № 42» и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.

Настоящая Политика вводится в действие приказом директора МБОУ «Гимназия № 42».

Политика признается утратившей силу на основании приказа директора МБОУ «Гимназия № 42».

Изменения в политику вносятся приказом директора МБОУ «Гимназия № 42». Инициаторами внесения изменений в политику информационной безопасности являются:

– директор МБОУ «Гимназия № 42»;

– работники административно-управленческого персонала МБОУ «Гимназия № 42»;

– администратор информационной безопасности.

Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация политики ИБ и производится в обязательном порядке в следующих случаях:

– при изменении политики Российской Федерации в области ИБ, указов и законов Российской Федерации в области защиты информации;

– при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ МБОУ «Гимназия № 42;

– при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб МБОУ «Гимназия № 42».

Ответственными за актуализацию политики ИБ (плановую и внеплановую) несет АИБ.

Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на АИБа.

3. Политики информационной безопасности МБОУ «Гимназия № 42»

3.1. Назначение политик информационной безопасности

Политики ИБ МБОУ «Гимназия № 42» – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в МБОУ «Гимназия № 42».

Под политиками безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политики ИБ относятся к административным мерам обеспечения ИБ и определяют стратегию МБОУ «Гимназия № 42» в области ИБ.

Политики ИБ регламентируют эффективную работу СЗИ. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политики ИБ реализуются посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Все документально оформленные решения, формирующие Политики, должны быть утверждены директором МБОУ «Гимназия № 42».

3.2. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

– постоянный и всесторонний анализ информационного пространства МБОУ «Гимназия № 42» с целью выявления уязвимостей информационных активов;

– своевременное обнаружение проблем, потенциально способных повлиять на ИБ МБОУ «Гимназия № 42», корректировка моделей угроз и нарушителя;

– разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей МБОУ «Гимназия № 42», а также повышать трудоемкость технологических процессов обработки информации;

– контроль эффективности принимаемых защитных мер;

– персонификация и адекватное разделение ролей и ответственности между сотрудниками МБОУ «Гимназия № 42», исходя из принципа персональной и единоличной ответственности за совершаемые операции.

3.3. Соответствие Политики безопасности действующему законодательству

Правовую основу политик составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.

3.4. Ответственность за реализацию политик информационной безопасности

Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

Ответственность за реализацию политик возлагается:

– в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты – на АИБа;

– в части, касающейся доведения правил политик до сотрудников МБОУ «Гимназия № 42», а также иных лиц (см. область действия настоящей политики) – на АИБа;

– в части, касающейся исполнения правил политики, – на каждого сотрудника МБОУ «Гимназия № 42», согласно их должностным и

функциональным обязанностям, и иных лиц, попадающих под область действия настоящей политики.

***3.5.* Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе**

Организация обучения сотрудников МБОУ «Гимназия № 42» в области ИБ возлагается на АИБа.

Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности».

Обучение проводится согласно Плану, утвержденному руководителем МБОУ «Гимназия № 42».

Обучение сотрудников МБОУ «Гимназия № 42» правилам обращения с конфиденциальной информацией, проводится путем:

- проведения администратором информационной безопасности инструктивных занятий с сотрудниками, принимаемыми на работу в МБОУ «Гимназия № 42»;
- самостоятельного изучения сотрудниками внутренних нормативных документов МБОУ «Гимназия № 42».

Допуск персонала к работе с защищаемыми ИР МБОУ «Гимназия № 42» осуществляется только после его ознакомления с настоящими политиками, а также после ознакомления пользователей с «Порядком работы пользователей» МБОУ «Гимназия № 42», а так же иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящих политик подтверждается подписями сотрудников в «Журнале проведения инструктажа по информационной безопасности».

Допуск персонала к работе с КИ МБОУ «Гимназия № 42» осуществляется после ознакомления с «Порядком организации работы с материальными носителями», «Порядком организации работы с электронными носителями». Правила допуска к работе с ИР лиц, не являющихся сотрудниками МБОУ «Гимназия № 42», определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

3.6. Защищаемые информационные ресурсы МБОУ «Гимназия № 42»

Различаются следующие категории информационных ресурсов, подлежащих защите в МБОУ «Гимназия № 42»:

Конфиденциальная – информация, определенная в соответствии с Федеральным Законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 29.07.2004г. № 98-ФЗ «О коммерческой тайне», ФЗ от 27.07.2006г. № 152-ФЗ «О персональных данных», указом президента РФ от 06.03.1997г. № 188 «Об утверждении перечня сведений конфиденциального характера», постановлением правительства РФ от 17.11.2007г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», предусмотренная Перечнем сведений конфиденциального характера.

Публичная – информация, получаемая из публичных источников (публикации в СМИ, теле и радиовещание и т.д.). Информация, предназначенная для размещения на внешних публичных ресурсах;

Открытая – информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят. Информация, сформированная в результате деятельности МБОУ «Гимназия № 42», которую запрещено относить конфиденциальной на основании законодательства России. Информация, представляемая в публичный доступ, используемая в хозяйственной деятельности МБОУ «Гимназия № 42» или имеющая принципиальное значение для имиджа МБОУ «Гимназия № 42»;

Ограниченного доступа – информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенной категории лиц.

Конфиденциальная информация представляет собой сведения ограниченного доступа, для которых в качестве основной угрозы безопасности рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

Защищаемые информационные ресурсы определяются в соответствии с «Перечнем защищаемых ресурсов», утверждаемым соответствующим приказом директором МБОУ «Гимназия № 42».

Подходы к решению проблемы защиты информации в МБОУ «Гимназия № 42», в общем виде, сводятся к исключению неправомерных или неосторожных действий со сведениями, относящимися к информации ограниченного распространения, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования производственных процессов МБОУ «Гимназия № 42».

Для этого в МБОУ «Гимназия № 42» выполняются следующие мероприятия:

- определяется порядок работы с документами, образцами изделиями и др., содержащими конфиденциальные сведения;
- устанавливается круг лиц и порядок доступа к подобной информации;
- вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные сведения;
- включаются в трудовые договоры с сотрудниками обязательства о неразглашении конфиденциальных сведений и определяются санкции за нарушения порядка работы с ними и их разглашение.

Форма подписки о неразглашении конфиденциальной информации подписывается при заключении трудового договора, который подписывается всеми сотрудниками учреждения при приеме на работу в МБОУ «Гимназия № 42». Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых МБОУ «Гимназия № 42» с другими организациями. Персональные данные сотрудника учреждения – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

Согласно ст. 86 п. 7 Трудового кодекса РФ защита персональных данных сотрудника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

Согласно ст. 88 Трудового кодекса РФ при передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

- осуществлять передачу персональных данных сотрудника в пределах одной организации в соответствии с локальным нормативным актом организации, с которым сотрудник должен быть ознакомлен под расписку;

- разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретных функций.

Согласно ст. 90 Трудового кодекса РФ лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

4. Политики информационной безопасности

4.1. Политика предоставления доступа к информационному ресурсу

4.1.1.Назначение

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым ИР МБОУ «Гимназия № 42».

4.1.2.Положение политики

Положения данной политики определены в «Положении о разрешительной системе допуска», утверждаемом соответствующим приказом директором МБОУ «Гимназия № 42».

4.2. Политика учетных записей

4.2.1.Назначение

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов МБОУ «Гимназия № 42».

4.2.2.Положение политики

Регистрационные учетные записи подразделяются на:

– пользовательские – предназначенные для идентификации/ аутентификации пользователей информационных активов МБОУ «Гимназия № 42»;

– системные – используемые для нужд операционной системы;

– служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов МБОУ «Гимназия № 42» назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

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

одной общей пользовательской учетной записи разными пользователями запрещено.

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

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

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

4.3. Политика использования паролей

4.3.1.Назначение

Настоящая Политика определяет основные правила парольной защиты в МБОУ «Гимназия № 42».

4.3.2.Положения политики

Положения политики закрепляются в «Порядке по организации парольной защиты».

4.4. Политика реализации антивирусной защиты

4.4.1.Назначение

Настоящая Политика определяет основные правила для реализации антивирусной защиты в МБОУ "Гимназия № 42".

4.4.2.Положения политики

Положения политики закрепляются в «Порядке по проведению антивирусного контроля».

4.5. Политика защиты автоматизированного рабочего места

4.5.1.Назначение

Настоящая Политика определяет основные правила и требования по защите информации МБОУ «Гимназия № 42» от неавторизованного доступа, утраты или модификации.

4.5.2.Положения политики

Положения данной политики определяются в соответствии с используемым техническим решением.

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными стандартами МБОУ «Гимназия № 42», (согласно занимаемой должности).

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратор информационной безопасности.

Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к корпоративной информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору, а все обращения должны регистрироваться.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных сетевых ресурсов или съемных носителей, маркированных отделом внедрения автоматизированных систем финансовых расчетов, и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками МБОУ «Гимназия № 42».

Запрещается использование указанных АРМ другими пользователями без согласования с заместителем директора по УВР. При передаче указанного АРМ другому пользователю, должна производится гарантированная очистка диска (форматирование).

Системный администратор вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

5. Профилактика нарушений политик информационной безопасности

Под профилактикой нарушений политик ИБ понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в МБОУ «Гимназия № 42» и проведение разъяснительной работы по ИБ среди пользователей.

Положения определены документами, утвержденными Приказом «Об обучении сотрудников правилам защиты информации», и «Порядком технического обслуживания средств вычислительной техники».

АИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР ИС рекомендуется уведомить АИБа, и далее следовать их указаниям.

Действия АИБа и администратора информационной системы при признаках нарушения политик информационной безопасности регламентируются следующими внутренними документами:

– регламентом пользователя;

– политикой информационной безопасности;

– регламентом администратора информационной безопасности;

– регламентом системного администратора.

После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

Ответственность за выполнение правил ПБ несет каждый сотрудник МБОУ «Гимназия № 42» в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования ПБ МБОУ «Гимназия № 42», могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный МБОУ «Гимназия № 42» в результате нарушения ими правил политики ИБ (ст. 238 Трудового кодекса Российской Федерации).

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 МБОУ «Гимназия № 42» несут ответственность в

соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

6. Регулирующие законодательные нормативные документы

При организации и обеспечении работ по ИБ сотрудники МБОУ «Гимназия № 42» должны руководствоваться следующими законодательными нормативными документами:

6.1. Основополагающие нормативные документы

К основополагающим нормативным документам относятся:

– конституция Российской Федерации (принята на всенародном голосовании 12.12.1993);

– концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов (разработана во исполнение Указа Президента Российской Федерации от 01.07.1994 N 1390 «О совершенствовании информационно-телекоммуникационного обеспечения органов государственной власти и порядке их взаимодействия при реализации государственной политики в сфере информатизации»);

– концепция национальной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 17.12.1997 N 1300, в редакции Указа Президента Российской Федерации N 24 от 10.01.2000);

– доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации от 09.09.2000 N Пр-1895).

6.2. Законы Российской Федерации

– Гражданский кодекс Российской Федерации.

– Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

– Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»;

– Закон Российской Федерации от 21.07.1993 N 5485-1 «О государственной тайне»;

– Федеральный закон от 07.07.2003 N 126-ФЗ «О связи»;

– Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ от 13.06.1996;

– Федеральный закон от 27.12.2002 N 184-ФЗ «О техническом регулировании»;

– Федеральный закон от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности».

6.3. Указы и распоряжения президента Российской Федерации

– Указ Президента Российской Федерации от 14.01.1992 N 20 «О защите государственных секретов Российской Федерации»;

– указ Президента Российской Федерации от 07.10.1993 N 1607 «О государственной политике в области охраны авторского права и смежных прав»;

– указ Президента Российской Федерации от 31.12.1993 N 2334 «О дополнительных гарантиях прав граждан на информацию»;

– указ Президента Российской Федерации от 20.01.1994 N 170 «Об основах государственной политики в сфере информатизации»;

– указ Президента Российской Федерации от 03.04.1995 N 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;

– указ Президента Российской Федерации от 03.07.1995 N 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации»;

– указ Президента Российской Федерации от 30.11.1995 N 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»;

– указ Президента Российской Федерации от 09.01.1996 N 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации»;

– указ Президента Российской Федерации от 16.08.2004 N 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;

– указ Президента Российской Федерации от 06.10.2004 N 1286 «Вопросы Межведомственной комиссии по защите государственной тайны»;

– указ Президента Российской Федерации от 06.03.1997 N 188 «Об утверждении перечня сведений конфиденциального характера»;

– распоряжение Президента Российской Федерации от 16.04.2005 N 151-рп «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне».

6.4. Постановления и распоряжения правительства Российской Федерации

– Постановление Правительства Российской Федерации от 03.11.1994 N 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

– постановление Правительства Российской Федерации от 26.01.2006 N 45 «Об организации лицензирования отдельных видов деятельности»;

– постановление Правительства Российской Федерации от 15.04.1995 N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»;

– постановление Правительства Российской Федерации от 29.12.2007 N 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;

– постановление Правительства Российской Федерации от 31.08.2006 N 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;

– постановление Правительства Российской Федерации от 26.06.1995 N 608 «О сертификации средств защиты информации»;

– постановление Правительства Российской Федерации от 04.09.1995 N 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»;

– постановление Правительства Российской Федерации от 15.08.2006 N 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;

– постановление Правительства Российской Федерации от 01.07.1996 N 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности».

6.5. Нормативные и руководящие документы Федеральных служб Российской Федерации

– Приказ ФСБ Российской Федерации от 09.02.2005 N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

– Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992);

– Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники (утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992);

– Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992);

– Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден

решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.);

– Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.);

– Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25.07.1997);

– Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.);

– Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 04.06.1999 N 114);

– Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (введен в действие приказом Гостехкомиссии России N 187 от 19.06.02 г.);

6.6. Государственные стандарты

– ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение» (утвержден постановлением Госстандарта СССР от 28.06.1984 N 2206);

– ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (утвержден постановлением Госстандарта СССР от 24.03.1989 N 661);

– ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят постановлением Госстандарта России от 09.02.1995 N 49);

– ГОСТ Р 50752-95 «Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний»;

– ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство» (введен в действие постановлением Госстандарта России от 14.07.1998 N 295);

– ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения»;

– ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования»;

– ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (принят постановлением Госстандарта России от 29.12.2005 N 447-ст).