ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННОГО УЧРЕЖДЕНИЯ ОБРАЗОВАНИЯ «СРЕДНЯЯ ШКОЛА №» Г. ЖЛОБИНА»

 Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика информационной безопасности государственного учреждения образования «Средняя школа №2 г. Жлобина» (далее – Политика) разработана на основании Закона Республики Беларусь «Об информации, информатизации и защите информации», Закона Республики Беларусь «О защите персональных данных» и иных нормативных правовых актов Республики Беларусь в области информационной безопасности.

1.2.Политика распространяется на работников и обучающихся государственного учреждения образования «Средняя школа №2 г. Жлобина» (далее – Школа, Учреждение), а также привлекаемых лиц, участвующих в эксплуатации (использующих в своей работе), обслуживании, поддержке объектов информационной системы (далее – ОИС), программного обеспечения (прикладного и системного) (далее – ПО), информационных ресурсов (далее – ИР), информационных систем (далее – ИС) Школы (собственных, либо предоставленных на договорной основе).

1.3.Настоящая Политика входит в состав документации на систему защиты информации информационной системы школы.

1.4. Общее руководство системой информационной безопасности (далее – ИБ), принятие всех решений по вопросам ее функционирования, а также контроль за организацией работы по обеспечению ИБ возлагается на директора. На заместителей директора возлагается ответственность за обеспечение ИБ по направлениям их деятельности в соответствии с распределением обязанностей.

1.5. Организационные и технические работы по обеспечению ИБ компьютерной сети и баз данных автоматизированных систем управления в школе выполняет инженер-программист в соответствии с локальными правовыми актами (далее – ЛПА), устанавливающими порядок осуществления деятельности по ИБ в школе. В школе обеспечивается наличие лиц, обладающих необходимой квалификацией и прошедших соответствующее обучение, а также повышение квалификации в установленном порядке.

Глава 2. ПРИНЦИПЫ И ЦЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Политика учреждения по обеспечению ИБ направлена на гармонизацию подходов и требований по обеспечению ИБ к работникам и обучающимся учреждения, государственным органам и организациям, а также юридическим и физическим лицам и индивидуальным предпринимателям (далее – субъекты информационных отношений) при осуществлении учреждением своей деятельности.

2.2. Основными целями Политики ИБ являются: снижение уровня рисков, связанных с ИБ; снижение числа инцидентов, связанных с ИБ;

2 повышение компетентности работников в области ИБ; улучшение имиджа учреждения и минимизация ущерба вследствие возможного возникновения инцидентов ИБ и кибербезопасности; обеспечение непрерывности бизнес-процессов; обеспечение соответствия требованиям законодательства, стандартам и договорным обязательствам в части ИБ и защиты персональных данных.

2.3. Достижение указанных целей осуществляется посредством выполнения следующих мероприятий: реализация требований законодательства Республики Беларусь в части ИБ и мер контроля их защищенности; определение ответственности субъектов информационных отношений (далее – Субъектов) по обеспечению и соблюдению требований Политики, в том числе с использованием ИР, ИС и ОИС, а также посредством принятия соответствующих внутренних ЛПА по обеспечению ИБ учреждения; своевременное выявление и оценка причин, условий и характера угроз ИБ, а также дальнейшее прогнозирование развития событий на основе мониторинга инцидентов ИБ; планирование, реализация и контроль эффективности использования мер и средств защиты информации, создание механизма оперативного реагирования на угрозы ИБ; повышение осведомленности и обучение работников учреждения возможным факторам рисков ИБ и мерам противодействия им.

 2.4. Построение системы защиты информации и ее функционирование должно осуществляться в соответствии со следующими принципами: законность: предполагает осуществление защитных мероприятий и разработку системы защиты информации учреждения в соответствии с действующим законодательством Республики Беларусь; системность: системный подход к построению системы защиты информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации; комплексность: комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты; непрерывность защиты: непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем; своевременность: предполагает упреждающий характер мер для обеспечения безопасности информации; преемственность и совершенствование: предполагают постоянное совершенствование мер и средств защиты информации; экономическая целесообразность: предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов по отношению к величине возможного ущерба; персональная ответственность: предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого работника в пределах его полномочий; принцип минимизации полномочий: означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью; научная обоснованность и техническая реализуемость: информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки 3 зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации; контроль: предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил безопасности.

Глава 3. СУБЪЕКТЫ, ОБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ И ПОРЯДОК ИХ ВЗАИМОДЕЙСТВИЯ

3.1. Субъектами информационных отношений являются: Школа, выступающая в качестве владельца информации и собственника имеющихся ИР, ИС и ОИС; государственные органы и организации; физические и юридические лица (индивидуальные предприниматели), в том числе иностранные, международные организации, выступающие в качестве информационных посредников, операторов информационных систем и связи, поставщиков ОИС, а также в качестве поставщика услуг учреждению, в том числе технической поддержки, гарантийного и сервисного обслуживания. 3.2. Субъектами в рамках учреждения являются внутренние и внешние пользователи: внутренние пользователи: работники, осуществляющие обеспечение безопасного использования ИР, ИС и ОИС; иные работники: педагогический состав школы, получивший доступ к ИР, ИС и ОИС школы и использующий их в рамках выполнения своих должностных обязанностей; внешние пользователи: должностные лица организаций, поставляющие ИР, ИС и ОИС для учреждения и осуществляющие их гарантийное и сервисное обслуживание.

3.3. Ответственность Субъектов информационных отношений за обеспечение защиты информации в учреждении установлена в следующих документах: организационно-распорядительных документах; должностных инструкциях работников учреждения, в обязанности которых входит обеспечение защиты ИС; иных документах, в том числе в иных локальных правовых актах, а также в соглашениях и договорах.

3.4. Объектами информационных отношений (далее – Объекты) являются: информация, хранящаяся и обрабатываемая в информационных системах учреждения, в том числе конфиденциальная и содержащая персональные данные; информационная инфраструктура, включающая ИР, ИС и ОИС.

3.5. Порядок информационного взаимодействия Объектов между собой определяется соответствующей эксплуатационной (технической) документацией.

3.6. Основными составляющими Объектами являются компоненты, входящие в состав информационной инфраструктуры учреждения: локальная сеть; информационные системы; отдельные рабочие места, предназначенные для доступа, хранения и обработки информации, не отнесенной к государственным секретам, распространение и (или) предоставление которой ограничено.

 Глава 4. РАЗГРАНИЧЕНИЕ ДОСТУПА К ОБЪЕКТАМ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

4.1. Субъекты имеют необходимый уровень доступа к Объектам учреждения, назначенный в соответствии с принципом минимизации прав, назначаемых пользователям. Доступ к информации и настройкам предоставляется в следующих случаях и в объёме: работникам ЦИТ предоставляется доступ к Объектам в соответствии с их ответственностью и полномочиями; иным работникам учреждения и педагогическому составу предоставляется доступ к Объектам в рамках выполнения ими соответствующих должностных обязанностей; лицам, поставляющим ОИС, а также осуществляющим их гарантийное, сервисное обслуживание и жизнеобеспечение, предоставляется доступ к Объектам в рамках договоров на оказание услуг; должностным лицам организаций в рамках Заявлений, Соглашений, Договоров; обучающимся учреждения предоставляются исключительно гостевой доступ к сетям, либо устройствам, с ограниченным доступом к ИС и ИР учреждения.

 4.2. Порядок и правила предоставления доступа к Объектам учреждения определяются следующими документами: настоящей Политикой; договорами при оказании учреждению услуг, в том числе технической поддержки; должностными и рабочими инструкциями работников; положением о ЦИТ; иными локальными правовыми актами учреждения.

4.3. Делопроизводство по документам, содержащим служебную информацию ограниченного распространения, регулируется существующим законодательством и ЛПА, содержащим служебную информацию ограниченного распространения.

4.4. Разграничение доступа к ИС и их Объектам осуществляется с помощью средств управления правами доступа к соответствующим активам. К указанным средствам относятся: групповые политики безопасности; средства управления доступом к операционной системе; средства управления доступом к официальному сайту школы и электронной почте; средства управления доступом к ИС, ИР, ОИС учреждения; средства управления доступом к базам данных учреждения; средства управления доступом к системам хранения данных учреждения; средства управления доступом к ИС и их Объектам, ИР, предоставленным пользователям в рамках выполнения должностных обязанностей и договорных отношений.

4.5. Разграничение доступа к вышеуказанным активам учреждения включает в себя: регистрацию и идентификацию пользователей; аутентификацию пользователей; авторизацию пользователей для получения доступа; регистрацию и учет попыток доступа к защищаемым активам.

 4.6. При определении полномочий каждого авторизованного пользователя выполняются следующие условия: полномочия пользователя соответствуют его должностным обязанностям и осуществляются только в границах этих полномочий; полномочия пользователя должны распространяться на конкретные категории информации, ИС и их Объектов, ИР.

4.7. С целью разграничения прав доступа работников к Объектам учреждения используются роли безопасности. В базовом варианте применяются следующие роли 5 безопасности: роль «Администратор» и «Пользователь». В случае необходимости более детального разграничения применяются дополнительные роли, в зависимости от конкретной ИС и ИР.

4.8. Назначение ролей пользователей информационной инфраструктуры учреждения осуществляется исходя из выполняемых ими должностных обязанностей. Для каждой роли в отношении единицы актива определен и (или) ограничен список допустимых операций. Допускается совмещение нескольких ролей одним работником по функциям, не оказывающим влияния на уровень безопасности объекта, в том случае, если эти роли не являются взаимоисключающими. Каждой роли соответствуют определенные права доступа Субъекта к Объекту – авторизованный пользователь. Ролевое деление авторизованных пользователей реализуется с помощью функциональных возможностей разграничения доступа к ИС и их Объектам, ИР. В случае предоставления пользователю новой роли его права доступа к защищаемым данным и информационной инфраструктуре учреждения пересматриваются. В случае увольнения (независимо от обстоятельств прекращения трудовых отношений) или перевода работника Школы в другое структурное подразделение либо на другую должность его права доступа пересматриваются или блокируются. В случае выявления инцидентов безопасности права доступа авторизированного пользователя блокируются (либо ограничиваются) до завершения рассмотрения инцидента.

4.9. ОИС (за исключением ПК и мобильных устройств, используемых в служебных целях вне территории школа) располагаются в помещениях, исключающих несанкционированный доступ к ним и обеспечивающих их бесперебойную круглосуточную эксплуатацию в климатических условиях, указанных в документации на эксплуатацию.

4.10. Работникам структурных подразделений, имеющим право доступа к обработке персональных данных, содержащихся в информационных системах (ресурсах) школы, обеспечивается право доступа к соответствующим ИС.

Глава 5. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ (ПОЛЬЗОВАТЕЛЕЙ) ИНФОРМАЦИОННЫХ СИСТЕМ

5.1. Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании Объектов информационных отношений имеют право: использовать ОИС для доступа к ИС и ИР, другим ОИС с целями поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления и пользования информацией; осуществлять иные действия в соответствии с должностными инструкциями и ЛПА школы.

5.2. Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании Объектов информационных отношений обязаны: соблюдать права других лиц при использовании Объектов школы; соблюдать надежность пароля (базовые требования: длина пароля - не менее восьми символов; алфавит - кириллица, латиница, цифры, специальные символы; плановая смена пароля - не реже одного раза в квартал) для предотвращения взлома; хранить пароль в месте, исключающем его компрометацию другими пользователями и иными лицами; запрещено предоставлять иным лицам пароль от личной учётной записи. Обладателем пароля к личной учётной записи является только его пользователь; запрещается переходить по активным ссылкам в письмах, полученных из неизвестных (ненадёжных) источников; исполнять обязанности в соответствии с должностными инструкциями и ЛПА школы; не допускать открытия гиперссылок из ненадёжных источников («зловредных ссылок») при использовании корпоративных и личных почтовых ящиков на рабочих местах; Запретить хранение и передачу паролей в открытом виде, использовать для хранения и передачи паролей специализированное ПО - менеджеры паролей.

 5.3. В групповых политиках доменов установить следующие требования к паролям: длина пароля не менее 12 символов для непривилегированных учётных записей и 16 символов для привилегированных учётных записей; пароль должен содержать заглавные буквы, строчные буквы, цифры, а также специальные символы: (! @#$%Л&\*() -\_ + = ~[] { } |\ ^: ; «» ?); пароль не должен совпадать со словарными словами, а также содержать личные данные пользователя, которые бы позволяли вычислить значение пароля, например: ФИО, номера телефонов, памятные даты (дни рождения и т.д.); последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.); общепринятые сокращения («USER», «TEST», «ADMIN» и т.п.); срок действия паролей: не более 90 дней.

5.4 Права и обязанности субъектов школы в сфере информационной безопасности регламентированы следующими документами: настоящей Политикой; Положением об обработке и защите персональных данных; Положением о ЦИТ; должностными и рабочими инструкциями работников Университета; иными локальными правовыми актами университета.

5.5. Учреждение обязуется постоянно совершенствовать систему ИБ, обеспечивать ресурсами, достаточными для достижения указанных в настоящей Политике целей.

Глава 6. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ОБЪЕКТОВ УЧРЕЖДЕНИЯ С ИНЫМИ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И СИСТЕМАМИ

6.1. Порядок взаимодействия Объектов школы с иными ИС определяется действующим законодательством и соответствующими документами по каждому взаимодействию.

6.2. Функционирование Объектов школы осуществляется с обновлением системного, прикладного ПО и антивирусных баз из доверенных источников.

6.3. Обновление баз средств защиты информации от действий вредоносного ПО и файлов осуществляется с периодичностью, установленной производителем антивирусного ПО.

6.4. Доступ к сети Интернет предоставляется только авторизованным сервисам и пользователям. 7

6.5. К авторизованным сервисам Учреждения относятся: обновление системного и прикладного ПО; обновление встроенного ПО технических средств; обновление баз средств защиты информации от действий вредоносного ПО и файлов.

6.6. Правила доступа к сетям общего пользования определены и регулируются настоящей Политикой.

6.7. При взаимодействии Объектов Учреждения с иными ИС, в случае необходимости, применяются средства защиты информации, имеющие сертификат соответствия, выданный в порядке, установленном законодательством.

Глава 7. ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ

7.1. Работники и обучающиеся Учреждения, а также привлекаемые лица, участвующие в эксплуатации, обслуживании, поддержке объектов ОИС, ПО, ИР, ИС Учреждения (собственных, либо предоставленных на договорной основе) несут персональную ответственность за соблюдение требований настоящей Политики.

7.2. Неисполнение или некачественное исполнение работниками Учреждения, обучающимися, пользователями ИС обязанностей по обеспечению ИБ может повлечь лишение доступа к информационным ресурсам, а также применение к виновным мер воздействия, вид и степень которых определяется установленным в Учреждении порядком либо требованиями действующего законодательства.

Глава 8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

 8.1. В развитие настоящей Политики могут приниматься локальные правовые акты школы.

8.2. В случае изменения действующего законодательства, а также Устава школы, настоящая Политика применяется в части, не противоречащей вновь принятым нормативным правовым актам, а также Уставу школы.

8.3. При необходимости внесении изменений в настоящую Политику, изменения в существующий документ не вносятся, она переиздается и утверждается заново.

8.4 Актуализация настоящей Политики осуществляется на периодической и внеплановой основе: периодическое (плановое) изменение настоящей Политики должно осуществляться не реже одного раза в 24 месяца; внеплановое изменение настоящей Политики может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

8.5 Ответственным за актуализацию настоящей Политики является заместитель директора по учебной работе Волкова Е.М.

8.6 Изменения в Политике информационной безопасности согласовываются с заместителем директора по учебной работе Волковой Е.М. утверждаются директором.

 8.7 Финансирование работ по реализации положений настоящей Политики осуществляется в рамках собственных средств учреждения.