УТВЕРЖДАЮ
Директор
_____ К.В.Багмет
Приложение №1 к приказу №26
от «29» апреля 2019 года

ПОЛИТИКА
информационной безопасности
ГАУ ДПО «Центр повышения квалификации и профессиональной переподготовки работников социальной сферы»

1. Термины и определения

АРМ	-	Автоматизированное рабочее место
БД	-	База данных
ИБ	-	Информационная безопасность
ИС	-	Информационная система
ЛВС	-	Локально - вычислительная сеть
МЭ	-	Межсетевой экран
НМД	-	Нормативно – методический документ
НСД	-	Несанкционированный доступ
ПДн	-	Персональные данные
ПО	-	Программное обеспечение
СВТ	-	Средство вычислительной техники
СКЗИ	-	Средство криптографической защиты информации
СЗИ	-	Средство защиты информации
Аудит информационной безопасности; (аудит ИБ)	-	Систематический, независимый и документируемый процесс получения свидетельств деятельности по обеспечению ИБ, установления степени выполнения критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии ИБ
Идентификация	-	Процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
Информационный актив	-	Информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Центра ДПО находящаяся в распоряжении Центра ДПО и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме
ИР (информационный ресурс)	-	База, файл с данными, документ, контракт, соглашение, системная документация, обучающие материалы и пр. информация в электронном виде
Инцидент информационной безопасности; (инцидент ИБ)	-	Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, т.е. реализацию нарушения свойств ИБ информационных активов
Область действия системы обеспечения информационной безопасности; (область	-	Совокупность информационных активов и элементов информационной инфраструктуры Центра ДПО

действия СОИБ)		
Пароли технологических учетных записей	-	Пароли: администратора домена, локального администратора сервера и рабочих станций, сетевых служб, администратора баз данных, администратора сетевого оборудования, администратора телекоммуникационного оборудования, администратора приложений и программного обеспечения, пароли приложений и активного сетевого оборудования
Пользователи	-	Центра ДПО, не наделенные правами администратора ИС или ИТ-сервиса о котором идет речь
Съемный внешний носитель	-	Дискета, флэш-карта, внешний жесткий диск, CD – ROM, DVD – ROM, мобильное устройство, карта памяти
Система информационной безопасности; (СИБ)	-	Совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение
Система менеджмента информационной безопасности; (СМИБ)	-	Часть менеджмента Центра ДПО, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ
Система обеспечения информационной безопасности; (СОИБ)	-	Совокупность СИБ и СМИБ Центра ДПО

2. Общие положения

Политика ИБ (далее – Политика) устанавливает цели, задачи и принципы в области ИБ, которыми руководствуется ГАУ ДПО «Центр повышения квалификации и профессиональной переподготовки работников социальной сферы» (далее – Центр ДПО) в своей деятельности.

Положения Политики распространяются на всех работников Центра ДПО, имеющих доступ к информационным ресурсам, активам и ИТ-инфраструктуре Центра ДПО, а также учитываются в отношениях с контрагентами (поставщиками, подрядчиками, потребителями, партнерами, консультантами, слушателями, преподавателями (тьюторами)) и т.д.).

Целями Центра ДПО в области ИБ являются:

– обеспечение соответствия требованиям законодательства и договорным обязательствам в части ИБ;

– повышение деловой репутации и корпоративной культуры Центра ДПО;

– достижение адекватности мер по защите от угроз ИБ;

– предотвращение и (или) снижение ущерба от реализации угроз ИБ.

Совокупность защитных мер, реализующих обеспечение ИБ Центра ДПО, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, составляет систему информационной безопасности (далее – СИБ) Центра ДПО.

Совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов, составляет систему менеджмента информационной безопасности (далее – СМИБ) Центра ДПО.

Совокупность СИБ и СМИБ составляет систему обеспечения информационной безопасности (далее – СОИБ) Центра ДПО.

В Центре ДПО применяется риск-ориентированное управление информационной безопасностью. Это значит, что необходимость применения и выбор мер защиты определяется в зависимости от результатов оценки рисков ИБ.

Анализ и оценка рисков нарушения ИБ в свою очередь основывается на идентификации активов Центра ДПО, на их ценности для целей и задач Центра ДПО, на моделях угроз и нарушителей информационных систем Центра ДПО.

Перечень информационных активов, модель угроз, модель нарушителя должны пересматриваться ежегодно либо при внесении существенных изменений в СИБ или при выявлении инцидентов по ИБ.

3. Система информационной безопасности

3.1. Управление доступом

Доступ к информационным активам работникам Центра ДПО предоставляется на основании документально оформленных заявок, согласованных с владельцами соответствующих информационных активов.

Владельцем всех активов ИС Центра ДПО является директор Центра ДПО, если в документах Центра ДПО не определены исключения.

Требования и процедуры управления доступом установлены в документе «Политика управления доступом к информационным ресурсам».

3.2. Допустимое использование ИС и ИТ-сервисов

Использование ИС и ИТ-сервисов в Центре ДПО, в том числе обращение к ресурсам сети Интернет, разрешается исключительно в служебных целях.

Каждому работнику Центра ДПО назначается персональная учетная запись для входа в автоматизированное рабочее место, в информационные системы и для электронной почты.

Доступ работников к ресурсам сети Интернет, электронной почте, другим ИС и ИТ-сервисам предоставляется в соответствии с «Политикой управления доступом к информационным ресурсам».

Требования и правила использования ресурсов ИС и ИТ-сервисов Центра ДПО установлены в документе «Политика допустимого использования ИТ».

3.3. Антивирусная защита

Для защиты от вредоносных программ и нежелательной корреспонденции в Центре ДПО применяются официально приобретенные средства антивирусной защиты.

Установка и управление средствами антивирусной защиты на автоматизированных рабочих местах и сервере осуществляется организацией, с которой заключен договор на оказание услуг.

Каждый работник Центра ДПО обязан выполнять правила эксплуатации антивирусного ПО на АРМ и требования антивирусной безопасности.

Правила эксплуатации антивирусного ПО и требования антивирусной безопасности установлены в документе «Политика антивирусной защиты».

3.4. Защита сетевого взаимодействия

Для защиты информации при сетевом взаимодействии должна обеспечиваться:

– безопасность взаимодействия информационных систем с внешними сетями;

– безопасный удалённый доступ к информационным ресурсам;

– шифрование информации, передаваемой по неконтролируемым каналам связи.

Безопасность информационных систем при взаимодействии с внешними сетями обеспечивается следующими средствами защиты информации:

– межсетевыми экранами на границе подключения к внешним сетям.

Безопасность информационных ресурсов при удаленном доступе с использованием неконтролируемых каналов связи обеспечивается следующими средствами защиты информации:

– средствами обеспечения удаленного доступа;

– межсетевыми экранами на границе подключения к внешним сетям.

3.5. Криптографическая защита информации

Для защиты информации, передаваемой по неконтролируемым каналам связи, в Центре ДПО используются средства криптографической защиты информации.

Средства криптографической защиты информации приобретаются или поставляются в комплекте с эксплуатационной документацией.

Должен осуществляется поэкземплярный учет используемых средств криптографической защиты, эксплуатационной и технической документации к ним, ключевых документов в журнале учета средств криптографической защиты информации.

Правила использования средств криптографической защиты в системе клиент-банк устанавливается «Политикой использования систем «клиент-банк» Центра ДПО». Правила использования средств криптографической защиты в других информационных системах определяется эксплуатационной документацией и организационно-распорядительными документами Центра ДПО.

3.6. Физическая защита информации

Всё оборудование, критичное с точки зрения ИБ (сетевое оборудование, сервер) находятся в отдельном помещении (далее – помещение ограниченного доступа), доступ в которое разрешен только работникам, имеющим соответствующий допуск.

Помещения ограниченного доступа оборудуются как минимум:

1) Устройством для опечатывания двери;

2) Системой пожаротушения.

Управление правами доступа в помещение и средствами физической защиты осуществляет директор Центра ДПО.

Ключевые носители, носители с резервными копиями, пароли технологических учетных записей и иная информация ограниченного доступа должна храниться в сейфах.

Доступ в помещение ограниченного доступа посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находиться в помещении только в присутствии работников, имеющих соответствующий допуск.

Запрещается выносить за границы офиса оборудование и ПО, являющееся собственностью Центра ДПО, без письменного разрешения директора Центра ДПО.

3.7. Защита персональных данных

Бизнес-процессы и технологические процессы, в рамках которых производится обработка персональных данных, должны соответствовать законодательству Российской Федерации в сфере защиты персональных данных.

3.8. Обеспечение бесперебойного функционирования информационных систем.

Бесперебойность функционирования информационных систем Центра ДПО обеспечивается:

1) дублированием компонентов критических информационных систем;

2) резервированием каналов связи в критичных информационных системах;

3) резервным копированием данных критичных систем и хранением их в отдельных помещениях;

4) разработкой комплекса мероприятий по восстановлению данных в аварийных (кризисных) ситуациях;

5) договором сопровождения с фирмами-разработчиками информационных систем и приложений.

Для каждой информационной системы, должно быть определено время восстановления в случае нештатной ситуации и определен ответственный работник за восстановление.

При построении и внедрении новых информационных систем должны учитываться элементы обеспечения непрерывности, такие как дублирование основных элементов системы, реализация резервного копирования баз данных и конфигураций комплексов.

3.9. Управление инцидентами ИБ

Процесс управления инцидентами ИБ состоит из следующих последовательных этапов:

1) обнаружение инцидента ИБ и его регистрация;

2) информирование об инцидентах ИБ;

3) классификация инцидентов ИБ;

4) реагирование на инциденты ИБ;

5) анализ причин и оценка результатов.

В случае возникновения инцидентов в области ИБ:

1) управление инцидентом ИБ осуществляет ответственный за информационную безопасность;

2) приказом руководителя назначается комиссия по расследованию инцидента ИБ из числа и ответственный за информационную безопасность уполномоченная расследовать детали происшествия;

3) расследование должно быть направлено на выявление причин возникновения инцидента ИБ и личности злоумышленника;

4) в случае необходимости, Центр ДПО может эскалировать процесс расследования на органы охраны правопорядка Российской Федерации путем официальных запросов;

5) после персонализации лица или организации, осуществивших злоумышленное деяние, руководство Центра ДПО в соответствии с законодательством Российской Федерации принимает меры по вынесению взыскания и/или возмещению ущерба виновником инцидента и/или недопущению продолжения осуществления договорных отношений с выявленным лицом/организацией.

4. Система менеджмента информационной безопасности

Менеджмент ИБ есть часть общего корпоративного менеджмента Центра ДПО, которая ориентирована на содействие достижению целей деятельности организации через обеспечение защищенности ее информационной сферы.

Для реализации и поддержания ИБ в Центре ДПО реализуются четыре группы процессов:

1) планирование СОИБ («планирование»);

2) реализация СОИБ («реализация»);

3) мониторинг и анализ СОИБ («проверка»);

4) поддержка и улучшение СОИБ («совершенствование»).

Указанные группы процессов составляют СМИБ Центра ДПО.

Для осознанного обеспечения ИБ требуется выполнение в рамках СМИБ деятельности со стороны руководства, направленной на инициирование, поддержание, анализ и контроль СОИБ Центра ДПО.

Решения о реализации и эксплуатации СОИБ должны утверждаться руководством Центра ДПО. Должны быть документально оформлены решения руководства:

1) об анализе и принятии остаточных рисков нарушения ИБ;

2) о планировании этапов внедрения и улучшения СОИБ;

3) о распределении ролей в области обеспечения ИБ;

4) о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований ИБ и снижение рисков ИБ;

5) о выделении ресурсов, необходимых для реализации и эксплуатации СОИБ.

Целью выполнения деятельности в рамках группы процессов «планирование» является запуск «цикла» СМИБ путем определения

первоначальных планов построения, ввода в действие и контроля СОИБ, а также определения планов по совершенствованию СОИБ на основании решений, принятых на этапе «совершенствование». Выполнение деятельности на стадии «планирование» заключается в определении/корректировке области действия СОИБ, формализации подхода к оценке рисков ИБ и распределении ресурсов, проведении оценки рисков ИБ и определении/коррекции планов их обработки.

Деятельность на этапе «планирование» должна включать:

1) Планирование мероприятий по улучшению СОИБ;

2) Планирование контроля СОИБ;

3) Планирование проведения обучения по вопросам ИБ.

Все разрабатываемые и организуемые программы по обучению и повышению осведомленности в области ИБ должны обладать следующими характеристиками:

1) целевой направленностью: каждое мероприятие должно преследовать конкретные цели, например, информирование о конкретной угрозе;

2) возможностью контролировать результаты программ: должна быть выделена качественная характеристика, позволяющая оценить результаты проведения обучения – тесты, сбор статистики о событиях, проверки рабочих станций.

Этап «реализация» выполняется по результатам выполнения этапов «планирование» и/или «совершенствование» и заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СОИБ, определенных на этапе «планирование», и/или реализации решений, определенных на этапе «совершенствование» и не требующих выполнения деятельности по планированию соответствующих улучшений.

В результате выполнения деятельности на этапе «реализация» должна создаваться отчетная документация (акты, журналы и т.п.), фиксирующая результаты деятельности.

Целью выполнения деятельности в рамках группы процессов «проверка» является обеспечение достаточной уверенности в том, что СОИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ, а также внутренним и/или внешним условиям функционирования Центра ДПО, связанным с ИБ. На этапе «проверка» необходимо осуществлять мониторинг и контроль используемых защитных мер, периодически выполнять самооценку ИБ и проводить аудит ИБ, анализировать функционирование СОИБ в целом, в том числе со стороны руководства. Результат выполнения деятельности на этапе «проверка» является основой для выполнения деятельности по совершенствованию СОИБ.

Мониторинг событий ИБ должен проводится в соответствии с «Политикой мониторинга информационной безопасности».

При возникновении инцидента, работник, ответственный за мониторинг СОИБ, должен самостоятельно принять решение о необходимости блокировки

действия или оставить ситуацию без изменений, чтобы получить возможность выяснить источник и причину инцидента.

Работник, ответственный за мониторинг СОИБ, обязан поставить в известность об инциденте работника, ответственного за информационную безопасность.

Дальнейшие действия по конкретной ситуации должны быть выполнены комиссией по расследованию инцидента ИБ, на основании внутренних документов Центра ДПО и действующего законодательства Российской Федерации.

Аудит информационной безопасности должен проводится в соответствии с «Политикой аудита информационной безопасности».

В результате выполнения деятельности на этапе «проверка» должна создаваться отчетная документация (акты, журналы и т.п.), фиксирующая результаты деятельности по проверке ИБ.

Группа процессов «совершенствование» включает в себя деятельность по принятию решений о реализации тактических и/или стратегических улучшений СОИБ. Указанная деятельность, т.е. переход к этапу «совершенствование», реализуется только тогда, когда выполнение процессов этапа «проверка» дало результат, требующий совершенствования СОИБ, либо в случае существенного изменения процессов Центра ДПО. При этом сама деятельность по совершенствованию СОИБ должна реализовываться в рамках групп процессов «реализация» и при необходимости – «планирование».

Результаты выполнения деятельности на этапе «планирование» должны документироваться в виде плана совершенствования СОИБ.