Утверждаю:
Директор
_____/Кузнецов С.А./
«03» апреля 2023 г.

ПОЛОЖЕНИЕ
об ответственном за обработку информации содержащей персональные данные (конфиденциальную информацию) в Профессиональном образовательном учреждении частном «Колледж менеджмента»

1. Общие положения

1.1. Ответственный за обработку информации, содержащей персональные данные (далее Ответственный), является сотрудником ПОУЧ «Колледж менеджмента» (далее - Учреждения).

1.2. Ответственный назначается приказом руководителя Учреждения.

1.3. Ответственный непосредственно подчиняется руководителю Учреждения и проводит мероприятия по защите персональных данных в интересах Учреждения.

1.4. Ответственный в своей деятельности руководствуется:

- Конституцией Российской Федерации, принятой народом Российской Федерации 12 декабря 1993 года;
- Федеральным законом от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Гражданским кодексом Российской Федерации Часть I от 30 ноября № 51-ФЗ;
- Трудовым кодексом Российской Федерации от 30 декабря 2001 г. № 97-ФЗ;
- Уголовным кодексом Российской Федерации от 13 июня 1996 г. № 63-ФЗ;
- Кодексом Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи";
- федеральным законом от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;
- Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
- Федеральным законом от 18 июля 2011 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам осуществления государственного контроля (надзора) и муниципального контроля»;
- Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом урегулировании»;
- Федеральным законом от 07 апреля 2013 г. № 99-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» и Федерального закона «О персональных данных»;
- Федеральным законом от 22 декабря 2008 г. № 262 «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»;
- Указом Президента Российской федерации от 6 марта 1997 г. № 188 «Об утверждении сведений конфиденциального характера»;
- Постановлением Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»;

- Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановлением Правительства РФ от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- «Методическими рекомендациями по обеспечению с помощью крипто-средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утв. ФСБ России 21 февраля 2008 г. N 149/54-144;

- Приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности;

- Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- Уставом Учреждения;
- Политикой информационной безопасности Учреждения;
- Локальными нормативными актами Учреждения по защите персональных данных;
- Правилами внутреннего трудового распорядка;
- Настоящим Положением;
-Действующими нормативно-правовыми актами Российской Федерации.

1.5. Деятельность Ответственного осуществляется согласно требованиям действующего законодательства и плана мероприятий по защите персональных данных Учреждения на год.

2. Задачи

На Ответственного за обработку информации содержащей персональные данные возложены следующие **задачи:**

2.1. Организация комплексной защиты объектов информатизации Учреждения, а именно:

-информационные ресурсы, представленные в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащие персональные данные субъектов Учреждения и субъектов, взаимодействующих с Учреждением в рамках трудовых или иных взаимоотношений, организаций, юридических и физических лиц;

-средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, локальные вычислительные

сети и корпоративные информационные системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления информационными, управленческими и технологическими процессами, системы связи и передачи данных, технические средства приёма, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорные устройства и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для реализации процессов ведения деятельности, обработки информации, содержащей персональные данные субъектов Учреждения и субъектов, взаимодействующих с Учреждением в рамках трудовых или иных взаимоотношений, организаций, юридических и физических лиц.

2.2. Организация защиты персональных данных субъектов Учреждения.

2.3. Разработка организационных мероприятий, обеспечивающих безопасность объектов защиты Учреждения, своевременное выявление и недопущение возникновения возможных угроз информационной безопасности.

2.4. Организация проведения работ по технической защите информации на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций Учреждения.

2.5. Реализация технических мер, обеспечивающих своевременное выявление и недопущение возникновения возможных угроз информационной безопасности.

2.6. Организация системы управления рисками информационной безопасности в Учреждении. Разработка предложений по ее совершенствованию.

2.7. Организация системы управления инцидентами информационной безопасности в Учреждении. Разработка предложений по её совершенствованию.

2.8. Руководство группой реагирования на инциденты информационной безопасности по расследованию инцидентов информационной безопасности Учреждения.

2.9. Методическое руководство системой обеспечения информационной безопасности Учреждения.

2.10. Организация контроля состояния и оценки эффективности системы обеспечения информационной безопасности.

2.11. Разработка предложений и организация мероприятий по совершенствованию системы обеспечения информационной безопасности. Внедрение в информационную инфраструктуру Учреждения современных методов и средств обеспечения информационной безопасности.

3. Обязанности

3.1. Ответственный за обработку информации содержащей персональные данные данных **обязан:**

Правовая защита:

-организовать получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности, обработку персональных данных и сохранность конфиденциальной информации;

-осуществлять периодическое обучение и повышение квалификации работников Учреждения в области информационной безопасности.

Оценка угроз и рисков:

-принимать участие в анализе влияния на информационную безопасность Учреждения применяемых в деятельности Учреждения технологий, а также внешних по отношению к Учреждению событий;

-осуществлять контроль выявления проблем обеспечения информационной безопасности, участвовать в проведении анализа причин их возникновения и прогнозирования их развития;

-участвовать в определении моделей угроз, выявлении, анализе и оценки значимых для Учреждения угроз информационной безопасности,

-участвовать в выявлении возможных негативных последствий для Учреждения, наступающих в результате проявления рисков информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Учреждения;

-участвовать в идентификации и анализе рисковых событий информационной безопасности;

-осуществлять руководство по оценке величины рисков информационной безопасности и выявлении рисков, неприемлемых для Учреждения;

-участвовать в оценке влияния защитных мер на цели основной деятельности Учреждения;

-участвовать в оценке затрат на реализацию защитных мер;

Разрешительная система защиты:

-организовать контроль доступа в здания и помещения Учреждения, предназначенные для обработки сведений конфиденциального и персонального характера;

-организовать разрешительную систему допуска работников к работам с документами и персональными данными;

-организовать регламентацию и управление доступом к программным и программно-техническим средствам и сервисам информационных систем Учреждения и информации, обрабатываемой в них;

Физическая, программная и программно-аппаратная защита:

-обеспечить физическую сохранность автоматизированной системы и дополнительного оборудования;

-осуществлять координацию работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи;

-участвовать в практической проверке функционирования мер защиты обработки персональных данных и конфиденциальной информации;

-организовать систему обеспечения бесперебойной работы информационной системы обработки персональных данных и сети связи;

-организовать систему информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;

-организовать систему обеспечения возобновления работы информационных ресурсов и сети связи после прерываний и нештатных ситуаций;

-организовать применение средств защиты от вредоносных программ; организовать применение средств обнаружения вторжений; организовать внедрение программных, программно-аппаратных средств криптографической защиты информации (при необходимости);

-организовать установку, настройку и эксплуатацию систем защиты информации в соответствии с организационно-распорядительными документами и эксплуатационной документацией;

-разрабатывать предложения по обеспечению финансирования работ по защите персональных данных, в том числе выполняемых по договорам.

Обработка персональных данных:

-принять участие в определении единого порядка хранения и обращения персональных данных, конфиденциальной информации (носителей информации);

-организовать проведение мероприятий по минимизации данных конфиденциального (персонального) характера, доступных работникам;

-организовать систему предотвращения несанкционированного изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;

-осуществлять контроль проверки машинных и ручных протоколов выполнения работ со стороны пользователей;

-организовать мероприятия по созданию пассивной и активной системы снижения вероятности несанкционированного получения информации в устной форме, а также системы выявления каналов несанкционированного получения информации;

-обеспечить соблюдение режима конфиденциальности при обработке персональных данных;

Инциденты информационной безопасности:

-осуществлять контроль сбора информации о событиях информационной безопасности;

-организовать выявление и анализ инцидентов информационной безопасности;

-принять участие в расследовании инцидентов информационной безопасности;

-осуществлять оперативное реагирование на инцидент информационной безопасности;

-обеспечить минимизацию негативных последствий инцидентов информационной безопасности;

-осуществлять оперативное доведение до руководства Учреждения информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;

-организовать выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;

-разработать предложение по пересмотру применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;

Контроль мероприятий информационной безопасности:

-участвовать в разработке плана мероприятий по защите конфиденциальной информации (персональных данных) Учреждения;

-осуществление контроля за выполнением мероприятий по защите персональных данных, анализ материалов контроля, выявление недостатков и нарушений. Разработка и реализация мер по их устранению;

-осуществлять контроль за выполнением плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите персональных данных, выполняемых контрагентами;

-осуществлять контроль обеспечение функционирования и безопасности крипто-средств (при необходимости);

-осуществлять хранение и контроль ведения журналов Учреждения в части касающейся.

4. Права

Ответственный за обработку информации, содержащей персональные данные, **имеет право:**

-осуществлять контроль за деятельностью структурных подразделений Учреждения по выполнению ими требований по защите персональных данных и других вопросов, входящих в компетенцию Ответственного. При выявлении нарушений требований по защите персональных данных составлять акты, докладные записки, отчёты для рассмотрения руководством Учреждения;

-принимать необходимые меры при обнаружении несанкционированного доступа к персональным данным, как внутри Учреждения, так извне, и докладывать о принятых мерах директору Учреждения с представлением информации о субъектах, нарушивших режим доступа;

-вносить на рассмотрение директора Учреждения предложения, акты, заключения о приостановлении работ в случае обнаружения каналов утечки (или предпосылок к утечке) информации ограниченного доступа;

-давать структурным подразделениям Учреждения обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного;

-запрашивать и получать от всех структурных подразделений Учреждения сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного;

-согласовывать проектную и другую техническую документацию на новые объекты Учреждения в части выполнения требований по защите персональных данных;

-составлять акты и другую техническую документацию о степени защищенности объектов информатизации;

-готовить предложения о привлечении к проведению работ по оценке эффективности защиты персональных данных на объектах Учреждения (на договорной основе) учреждений и организаций, имеющих лицензию на соответствующий вид деятельности, а также предложения о закупке необходимых технических средств защиты и другой спецтехники, имеющих в обязательном порядке сертификат качества;

-рассматривать применяемые и предлагаемые методы защиты информации, промежуточных и конечных результатов исследований и разработок;

-представлять интересы Учреждения при осуществлении государственного контроля и надзора за обработкой персональных данных уполномоченным органом по защите прав субъектов персональных данных.

5. Взаимодействие

5.1. Ответственный за обработку информации, содержащей персональные данные, выполняет свои задачи во взаимодействии со всеми структурными подразделениями Учреждения.

5.2. Для выполнения своих функций и реализации предоставленных прав ответственный за обработку информации, содержащей персональные данные, взаимодействует с территориальными и региональными подразделениями Федеральной службы по техническому и экспортному контролю, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, ФСБ России, МВД России, другими представителями исполнительной власти и организациями, предоставляющими услуги и выполняющими работы в области защиты персональных данных на законном основании.

6. Ответственность

6.1. Ответственность за надлежащее и своевременное выполнение функций, предусмотренных настоящим Положением, несёт **лично** ответственный за обработку информации, содержащей персональные данные.

6.2. На Ответственного возлагается персональная ответственность за:

- обеспечение сохранности принятых на ответственное хранение документов и материальных средств; ,
- соблюдение правил пожарной безопасности;
- своевременное, а также качественное исполнение документов и поручений руководства Учреждения;
- обеспечение сохранности принимаемой и достоверность передаваемой информации;
- недопущение использования информации в неслужебных целях;
- организация контроля за режимом доступа к персональным данным.