Автономная некоммерческая организация
профессионального образования
«КОЛЛЕДЖ ПРАВОСУДИЯ»
(АНО ПО «Колледж правосудия»)

390046, г. Рязань, ул. Есенина, д. 116/1, офис 610, тел. (4912) 44-25-86,
e-mail: college-pravosudiya@mail.ru, rzn_apu@mail.ru, сайт: https://collegepravosudiya.ru/

УТВЕРЖДАЮ
Директор
АНО ПО «Колледж правосудия»
_____
К.А. Махиборода
«28» апреля 2023 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Автономной некоммерческой организации профессионального образования «КОЛЛЕДЖ ПРАВОСУДИЯ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 7E0FF2007BAE61B5454CD1C22EE32276
Владелец: МАХИБОРОДА КРИСТИНА АНДРЕЕВНА
Действителен: с 18.04.2022 до 18.07.2023

Рязань 2023

1. Основные термины и сокращения.

В Политике информационной безопасности АНО ПО «Колледжа правосудия» используются следующие основные термины и сокращения:

1) Автономная некоммерческая организация профессионального образования «КОЛЛЕДЖ ПРАВОСУДИЯ» (далее - «АНО ПО «Колледж правосудия», «Колледж») - образовательная организация профессионального образования, осуществляющая образовательную и научную деятельность, созданная для осуществления образовательных, научных, социальных и иных функций некоммерческого характера;

2) информация - сведения (сообщения, данные) независимо от формы их представления;

3) информационная безопасность - состояние защищённости информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам АНО ПО «Колледжу правосудия» и его работникам;

4) безопасность информации - состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;

5) защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо;

6) защита информации - принятие правовых, организационных и технических мер, направленных на:

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации;

7) инцидент информационной безопасности - появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности;

8) информационные ресурсы - документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках, базах данных, интернет-ресурсах, других информационных системах), зафиксированные в любой форме, на любом носителе информации;

9) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

10) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств защиты информации;

11) технические (аппаратные) средства защиты информации - это различные по типу устройства (механические, электромеханические, электронные и др.), которые на уровне оборудования решают задачи информационной защиты, например, такую задачу, как защита помещения прослушивания;

12) информационное пространство - совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры;
13) Информационная инфраструктура — система организационных структур, подсистема, обеспечивающая функционирование и развитие информационного пространства страны и средств информационного взаимодействия;
14) информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
15) системы и сети — информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, информационно-телекоммуникационные инфраструктуры центров обработки данных и облачных инфраструктур;
16) обладатель информации — лицо, самостоятельно создавшее информацию, либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
17) доступ к информации - возможность получения информации и её использования;
18) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя;
19) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
20) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
21) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
22) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях её материальный носитель;
23) электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;
24) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в её базах данных;
25) Интернет - глобальная информационно-телекоммуникационная сеть, связывающая информационные системы и сети электросвязи различных стран посредством глобального адресного пространства, основанная на использовании комплексов интернет-протоколов (Internet Protocol, IP) и протокола передачи данных (Transmission Control Protocol, TCP) и предоставляющая возможность реализации различных форм коммуникации, в том числе размещения информации для неограниченного круга лиц;
26) идентификация - совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимых для определения такого лица (далее - идентификатор);

27) аутентификация — совокупность мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификатором (идентификаторами) посредством использования аутентифицирующего (аутентифицирующих) признака (признаков) в рамках процедуры аутентификации, в результате чего лицо считается установленным;
28) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
29) автоматизированная обработка персональных данных - организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей потребителей информации;
30) распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
31) предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
32) блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
33) уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
34) материальный носитель информации машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека, на основе которых можно установить его личность;
35) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
36) субъект персональных данных — физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;
37) 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;
38) владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи;

39) ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Список нормативных правовых актов Российской Федерации, регламентирующих вопросы информационной безопасности

1. Конституция Российской Федерации.
2. Гражданский кодекс Российской Федерации.
3. Уголовный кодекс Российской Федерации.
4. Трудовой кодекс Российской Федерации.
5. Кодекс Российской Федерации об административных правонарушениях.
6. Доктрина информационной безопасности Российской Федерации, утверждённая Указом Президента Российской Федерации от 05.12.2016 № 646.
7. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28.01.1981).
8. Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
9. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
11. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
12. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
13. Указ Президента РФ от 20.01.1994 № 170 «Об основах государственной политики в сфере информатизации».
14. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».
15. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационныхсетей международного информационного обмена».
16. Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».
17. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
18. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
19. Постановление Правительства РФ от 26.06.1995№ 608 «О сертификации средств защиты информации».
20. Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
21. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

22. Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
23. Постановление Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
24. Постановление Правительства РФ от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации».
25. Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ- 2005)».
26. Приказ ФСБ России от 10.07.2014 № 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».
27. Приказ ФСБ РФ и Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. N 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».
28. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
29. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
30. Приказ ФСТЭК России от 21.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».
31. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
32. Приказ Федеральной службы по техническому и экспортному контролю от 29 апреля 2021 г. N 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».
33. Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 10 сентября 2021 г. N 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации».

34. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
35. Приказ ФСБ России от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных»

2. Общие положения

2.1. Политика информационной безопасности АНО ПО «Колледжа правосудия» (далее - «Политика») является документом, предназначенным для выражения позиции Колледжа в области информационной безопасности, при осуществлении в Колледже образовательной, научной, административно-хозяйственной, международной, и иной деятельности, определяющим систему взглядов, правила, принципы и подходы для обеспечения защищенности информационного пространства от внутренних и внешних угроз, способных нанести ущерб интересам Колледжа.
2.2. Политика разработана с учётом требований Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации в области информационной безопасности.
2.3. Политика распространяется на всё информационное пространство, в рамках деятельности Колледжа, включая охраняемую законом информацию (персональные данные, служебную тайну, в том числе учебную деятельность, сведения о сущности результатов интеллектуальной деятельности, выполнение научно-исследовательских работ и т.п.), за исключением государственной тайны.
2.4. Требования Политики распространяются на всех работников (основных и совместителей), обучающихся (студентов) и контрагентов Колледжа (далее- «работники, обучающиеся и контрагенты») и иных лиц, взявших на себя обязательства о неразглашении конфиденциальной информации, в порядке и на условиях, предусмотренных Политикой, законодательными и иными нормативными правовыми актами Российской Федерации и локальными нормативными актами Колледжа.
2.5. Положения Политики служат основой для разработки локальных нормативных актов (регламентов, инструкций и т.п.), регламентирующих вопросы информационной безопасности в Колледже.
2.6. Ответственность за организацию обеспечения безопасности персональных данных несут уполномоченные лица Колледжа, назначаемые приказом директора Колледжа.
2.7. Должностные лица Колледжа организуют и обеспечивают выполнение требований информационной безопасности во вверенных им подразделениях.
2.8. Работники, обучающиеся и контрагенты Колледжа обязаны соблюдать порядок обращения с конфиденциальными сведениями, ключами электронной подписи и иной защищаемой информаций, соблюдать требования Политики и других документов, регламентирующих в Колледже вопросы обеспечения информационной безопасности.
2.9. Политика является локальным нормативным актом Колледжа постоянного действия, которая вводится в действие, утверждается, изменяется и признаётся утратившей силу приказом директора Колледжа.

3. Цели и задачи Колледжа в области информационной безопасности

3.1. Целями Политики являются:

3.1.1. Формирование безопасного информационного пространства для функционирования и развития Колледжа, защита целостности деловой информации с целью поддержания возможности Колледжа по оказанию услуг высокого качества и принятию эффективных решений, при осуществлении образовательной, научной, административно - хозяйственной, международной и иной деятельности.

3.1.2. Снижение уровня рисков и угроз информационной безопасности до приемлемого уровня, позволяющего осуществлять устойчивое функционирование и развитие Колледжа.

3.1.3. Повышение осведомлённости работников в области рисков, связанных с информационными ресурсами Колледжа (обучение грамотности в области информационной безопасности, повышение квалификации и т.п.).

3.1.4. Определение степени ответственности и обязанностей работников по обеспечению информационной безопасности.

3.2. Для достижения целей Политики Колледжа обеспечивается решение следующих задач:

1) назначение и распределение функциональных прав и обязанностей между работниками Колледжа;

2) защита информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры, а также хранения в бумажном и электронном видах;

3) управление доступом к объектам информационной инфраструктуры:

- организация и контроль использования учётных записей;
- организация и контроль предоставления, отзыва и блокирование доступа;
- идентификация, аутентификация, авторизация (разграничение доступа) субъектов доступа к защищаемой информации;
- организация управления и защиты идентификационных и аутентификационных данных;
- организация и контроль физического доступа к объектам информационной инфраструктуры, местам хранения конфиденциальных документов;
- организация учёта и контроль состава ресурсов и объектов доступа;
- контроль целостности и защищённости информационной инфраструктуры Колледжа;

4) организация защиты от воздействий вредоносного кода (антивирусная защита);

5) предотвращение утечек информации;

6) организация защиты вычислительных сетей:

- сегментация и межсетевое экранирование вычислительных сетей;
- защита внутренних вычислительных сетей при взаимодействии с сетью Интернет;
- регистрация событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей;
- мониторинг и контроль содержимого сетевого трафика (выявление сетевых вторжений и атак);
- защита информации, передаваемой по вычислительным сетям;

7) безопасное использование ресурсов электронной корпоративной почты;

8) криптографическая защита информации;

9) защита информационных процессов, в рамках которых обрабатываются персональные данные;

10) использование взаимоувязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации;
11) управление деятельностью подразделения (работников), ответственного (ответственных) за организацию и контроль обеспечения защиты информации;
12) оценка и обработка рисков нарушения информационной безопасности;
13) организация и реализация мер по обучению и повышению квалификации работников в области обеспечения защиты информации;
14) управление инцидентами информационной безопасности: мониторинг, обнаружение и реагирование на инциденты информационной безопасности, их анализ;
15) организация обеспечения непрерывности деятельности информационных процессов Колледжа и их восстановления после преднамеренных либо непреднамеренных сбоев;
16) мониторинг состояния и контроль защитных мер информационной безопасности;
17) проведение аудита (оценки соответствия, самооценки) информационной безопасности и анализ функционирования системы ее обеспечения;
18) определение, классификация информационных ресурсов, подлежащих защите, определение их ценности и степени тяжести последствий от потери свойств информационной безопасности;
19) определение и актуализация списков возможных негативных воздействий на защищаемые ресурсы, способов реализации и степени вероятности реализации угроз информационной безопасности (модель угроз безопасности).
3.3. Требования Политики распространяются на всю конфиденциальную информацию Колледжа и ресурсы её обработки, независимо от формы их представления и вида носителя (бумажный, электронный и т.п.), на котором они зафиксированы.
3.4. Колледжа является правообладателем всей деловой информации и вычислительных ресурсов, приобретённых (полученных) и введённых в эксплуатацию в целях осуществления деятельности в соответствии с действующим законодательством. Указанные права распространяются в том числе на голосовую и факсимильную связь, осуществляемые с использованием оборудования Колледжа, программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех подразделений и работников Колледжа, созданные (полученные) в рамках исполнения трудовых обязанностей.

4. Основные принципы обеспечения информационной безопасности

4.1. Политика направлена на обеспечение непрерывного и безопасного функционирования его информационной среды, предотвращения несанкционированного доступа к защищаемым ресурсам, ненадлежащего их использования, в том числе разглашения, дублирования, изменения или удаления защищаемой информации.
4.2. Эффективная защита конфиденциальных сведений в информационном пространстве обеспечиваются следующими основными принципами:
1) постоянный и всесторонний анализ информационного пространства Колледжа в целях выявления уязвимостей информационных ресурсов на всех этапах их жизненного цикла;
2) своевременное обнаружение проблем и слабых мест, потенциально способных повлиять на информационную безопасность Колледжа, и нарушителя(ей), разработка и своевременная корректировка модели угроз информационной безопасности;
3) разработка и внедрение защитных мер (организационно-правовых, технических, программных), адекватных характеру выявленных угроз, с учётом затрат на их реализацию;

4) оценка эффективности принимаемых защитных мер;
5) персонификация и адекватное разделение ролей и ответственности между работниками Колледжа исходя из принципа персональной ответственности за совершаемые операции.
4.3. Доступ работников, обучающихся и контрагентов к конфиденциальным сведениям основывается на принципе «минимальности и достаточности», то есть каждому пользователю предоставляются наименьшие из возможных, но достаточные для выполнения служебных обязанностей, права доступа.
4.4. Доступ к конкретной конфиденциальной информации предоставляется только по согласованию с обладателем такой информации.

5. Объекты информационной безопасности. Сведения, подлежащие защите.

5.1. Основные объекты информационной безопасности
5.1.1. К основным объектам информационной безопасности в Колледжа, подлежащих защите, относятся: информационные ресурсы с ограниченным доступом, персональные данные, учебная деятельность, сведения о сущности результатов интеллектуальной деятельности, сведения о выполнении научно-исследовательских, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления.
5.2. Персональные данные.
5.2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
5.2.2. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.
5.2.3. Сведения о субъекте персональных данных в любое время исключаются из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.
5.3. Служебная тайна.
5.3.1. Служебная тайна - это конфиденциальные сведения (служебная информация, информация для служебного пользования и т.п.), доступные конкретным работников Колледжа, которые работают непосредственно с ними в силу своих должностных обязанностей и распространение которой ограничено в силу служебной необходимости на основании решения уполномоченного лица.
5.3.2. К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности Колледжа, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в Колледж несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.
5.3.3. К служебной информации относятся сведения, не подлежащие опубликованию в средствах массовой информации, использованию в открытых документах, оглашению на конференциях, переговорах, выставках и т.д.
5.3.4. Не могут быть отнесены к служебной информации ограниченного распространения:

1) акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
2) сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования работников, граждан и населения в целом, а также производственных объектов;
3) описание структуры Колледжа, его функций, направлений и форм деятельности, а также его адрес;
4) сведения о численности о составе работников Колледжа, о системе оплаты труда, об условиях труда, в том числе об охране труда.
5) порядок рассмотрения заявлении и обращений граждан и юридических лиц;
6) решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;
7) документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах Колледжа, необходимые для реализации прав, свобод и обязанностей граждан.
5.3.5. На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования».
5.3.6. Относить служебную информацию Колледжа к разряду ограниченного распространения может Директор Колледжа и его заместители.
5.3.7. Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения.
5.3.8. Служебная информация ограниченного распространения без санкции соответствующего должностного лица не подлежит разглашению (распространению).
5.4. Ключ электронной подписи.
5.4.1. Использование электронных подписей осуществляется при совершении гражданско-правовых сделок, при совершении иных юридически значимых действий.
5.4.2. Принципами использования электронной подписи являются:
1) право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями её использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;
2) возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» применительно к использованию конкретных видов электронных подписей;
3) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно^ с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.
5.4.3. Видами электронных подписей являются:

1. Простая электронная подпись - электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.
2. Неквалифицированная электронная подпись - электронная подпись, которая:
получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
создается с использованием средств электронной подписи.
3. Квалифицированная электронная подпись — электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам: ключ проверки электронной подписи указан в квалифицированном сертификате; для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».
5.4.4. Ключи электронной подписи также относятся к информационным ресурсам, требующим защиты. Порядок их выдачи, хранения, работы и передачи требуют соблюдения действующих законодательных норм и персональной ответственности каждого владельца.
5.4.5. Порядок выдачи, хранения, работы и передачи ключей электронной подписи осуществляется регламентом Колледжа об электронной подписи.
5.5. Организация работы с конфиденциальными сведениями. Ответственность должностных лиц н подразделений
5.5.1. Организация работы работников, обучающихся и контрагентов Колледжа с вышеуказанными конфиденциальными сведениям закрепляется в соответствующих положениях (инструкциях и т.п.), в которых также отражаются: перечень сведений, составляющих тайну; порядок доступа к ним; организация сохранности сведений; условия их использования; порядок передачи и предоставления данной информации; срок действия режима соответствующей тайны и т.д.
5.5.2. Указанные положения (инструкции и т.п.) разрабатываются подразделениями Колледжа (должностными лицами), ответственными за организацию работы и защиту конкретных информационных ресурсов в Колледже.
5.5.3. На основании вышеуказанных положений (инструкций и т.п.) могут разрабатываться свои внутренние нормативные документы по работе с конкретными защищаемыми сведениями, если это диктуется служебной необходимостью и спецификой работы с ними.
5.5.4. При заключении договора (трудового или ГПХ) работники/контрагенты подписывают соглашение об обязанности обеспечения охраны персональных данных, договор (трудовой или ГПХ) содержит информацию об обязанности обеспечения сохранности данных, составляющих служебную и иную охраняемую законом тайну, обладателем которой являются Колледж и (или) его контрагенты, а также ответственность за её разглашение.
5.5.5. Ответственность за организацию выполнения требований настоящей Политики, организацию работы и защиты конфиденциальной информации в структурных подразделениях возлагается на их руководителей.

6. Угрозы информационной безопасности

6.1. Основными видам угроз информационной безопасности в Колледже являются:

1) нарушение конфиденциальности («утечка информации») - реализуется в том случае, если информация становится известной лицу, не располагающему полномочиями доступа к ней. Угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой защищаемой информации, хранящейся в информационной системе или передаваемой от одной системы к другой;

2) нарушение целостности - реализуется при несанкционированном изменении информации, хранящейся в информационной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных);

3) нарушение доступности (отказа службы - реализуется, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Блокирование может быть постоянным - запрашиваемый ресурс никогда не будет получен, или может вызывать только задержку запрашиваемого ресурса.

6.2. Оценка угроз информационной безопасности в Колледже носит систематический характер и осуществляется как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии (модернизации) систем и сетей. Систематический подход к оценке угроз безопасности информации позволяет поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов, компонентов систем и сетей.

6.3. Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

а) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

б) инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

в) определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

г) оценка сценариев реализации угроз безопасности информации в системах и сетях, определение их актуальности, вероятности и степени воздействия на них.

6.4. Оценка угроз безопасности информации проводится Директором Колледжа и администратором баз данных с участием подразделений или специалистов, ответственных за эксплуатацию систем и сетей, основных (профильных) подразделений Колледжа.

6.5. Для оценки угроз информационной безопасности Колледжа могут привлекаться в установленном порядке специалисты сторонних организаций.

7. Ответственность за невыполнение требований информационной безопасности.

7.1. Общее руководство обеспечением информационной безопасности осуществляет директор Колледжа.

7.2. Руководители структурных подразделений несут персональную ответственность за защиту информации во вверенных им подразделениях, обязаны незамедлительно сообщать Директору обо всех инцидентах, связанных с нарушениями требований информационной безопасности.

7.3. Каждый работник, обучающийся, контрагент и иные лица, указанные в п. 2.4 настоящего Положения, несут персональную ответственность за обеспечение информационной безопасности при выполнении должностных и функциональных обязанностей, а также договорных обязательств.
7.4. Нарушение требований Политики, локальных нормативных актов по обеспечению информационной безопасности является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами, договорами, заключёнными между Колледжом и работниками.
7.5. В случае нарушения установленных правил, работники, обучающиеся и контрагенты могут быть ограничены в правах доступа к защищаемым ресурсам информационной среды Колледжа, а также привлечены к уголовной, административной, гражданско-правовой и дисциплинарной ответственности.

8. Порядок пересмотра Политики

8.1. Пересмотр Политики производится не реже одного раза в три года с целью приведения в соответствие определённых Политикой защитных мер реальным условиям и текущим требованиям к защите информации.
8.2. Внеплановое внесение корректив в настоящую Политику может производится по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер по защите информационных ресурсов, результатам проведения аудита информационной безопасности и других контрольных мероприятий.
8.3. Ответственность за осуществление контроля выполнения требований положений Политики, а также за поддержание данного документа в актуальном состоянии, несёт директор Колледжа.

9. Заключительные положения

9.1. Политика является общедоступным документом.
9.2. Требования Политики могут развиваться другими внутренними нормативными документами Колледжа, которые её дополняют и уточняют.
9.3. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Колледжа, настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам.