Министерство образования и науки Республики Башкортостан
ГАПОУ Стерлитамакский колледж строительства и профессиональных технологий

ЛА-03-176-2020

ПРИНЯТО:

На заседании Управляющего Совета колледжа

Протокол №4 от 17.11.2020 г.

УТВЕРЖДАЮ

Директор ГАПОУ СКСиПТ

_____ И.М. Гумеров

«17» 11 2020 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
00FD53FF2F32B0C36B1D79BF645EE30109
Владелец: Гумеров Ильдар Мунирович
Действителен: с 21.10.2022 до 14.01.2024

ПОЛОЖЕНИЕ
об информационной безопасности в ГАПОУ СКСиПТ

1. ОБЩИЕ ПОЛОЖЕНИИ

1.1. Настоящее Положение об информационной безопасности (далее – Положение) государственного автономного профессионально образовательно учреждения Стерлитамакский колледж строительства и профессиональных технологий (далее – колледж) является официальным документом.

1.2. Целью настоящего Положения является обеспечение безопасности объектов защиты Университета от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных (УБПДн).

1.3. Данное Положение разработано в соответствии с:

- Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.);
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федеральным законом от 29.12.2010 № 436 «О защите детей от информации, причиняющий вред их здоровью и развитию».
- И иными документами в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, к используемой в образовательном процессе информационной продукции.

1.4. Под информационной безопасностью образовательной организации следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

1.5. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.6. К объектам информационной безопасности в колледже относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. персональные данные;
- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.7. Система информационной безопасности (далее - СИБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата):
- целостность (точность и полноту информации и компьютерных про-
- грамм);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.8. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая зашита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная зашита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

1.9. Требования настоящего Положения распространяются на всех сотрудников колледжа, студентов колледжа, а также всех прочих лиц (подрядчики, аудиторы и т.п.).

2. ПРАВОВЫЕ НОРМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Образовательная организация имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников колледжа, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

2.2. Образовательная организация обязана обеспечить сохранность конфиденциальной информации.

2.3. Администрация колледжа:

- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- назначает ответственного за обеспечение информационной безопасности;
- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
- имеет право включать требования по защите информации в договоры по всем видам деятельности;
- разрабатывает перечень сведений конфиденциального характера;
- имеет право требовать защиты интересов образовательной организации со стороны государственных и судебных инстанций.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора образовательно учреждения (далее ОУ) о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников колледжа и др.

2.5 Порядок допуска сотрудников образовательной организации к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и образовательной организации об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Для обеспечения информационной безопасности в образовательной организации требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности колледжа;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся колледжа;
- учет всех носителей конфиденциальной информации.

4. ОРГАНИЗАЦИЯ РАБОТЫ С ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И ТЕХНОЛОГИЯМИ

4.1. Система организации делопроизводства:
- учет всей документации образовательной организации, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов колледжа в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

4.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

4.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

4.2.2. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

4.2.3. Выданные для работы дела и документы с грифом "Для служебного пользования" ("Ограниченного пользования") подлежат возврату в канцелярию в тот же день.

4.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.

4.2.5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы колледжа.

4.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

4.3. Для организации делопроизводства приказом директора колледжа назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором образовательной организации. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ НА ОБУЧАЮЩЕМ ПОРТАЛЕ КОЛЛЕДЖА

5.1. Портал колледжа относится к группе многопользовательских информационных систем с разными правами доступа.

5.2. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных.

5.3. Портал колледжа обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения.

5.4. Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой на портале колледжа.

5.5. Регламент общих ограничений для участников образовательного процесса при работе с порталом колледжа, обеспечивающим предоставление Услуги.

5.6. Участники образовательного процесса, имеющие доступ к порталу колледжа, не имеют права передавать персональные логины и пароли для входа на портал другим лицам.
5.7. Передача персонального логина и пароля для входа на портал колледжа другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.
5.8. Участники образовательного процесса, имеющие доступ к порталу колледжа, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).
5.9. Участники образовательного процесса, имеющие доступ к порталу колледжа, в случае нарушения конфиденциальности условий доступа в личный кабинет, уведомляют в течение не более чем одного рабочего дня со дня получения информации о таком нарушении руководителя ОО, службу технической поддержки портала.
5.10. Все операции, произведенные участниками образовательного процесса, имеющими доступ к порталу колледжа, с момента получения информации руководителем ОО и службой технической поддержки о нарушении, указанном в предыдущем абзаце, признаются недействительными.
5.11. При проведении работ по обеспечению безопасности информации в портале колледжа участники образовательного процесса, имеющие доступ к порталу, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.

РАЗРАБОТАНО:		27.11.2020	Руководитель отдела информационно-технического обеспечения А.Р. Валеев
	подпись	дата	ФИО
СОГЛАСОВАНО:		27.11.2020	Лицо, ответственное за оценку качества О.А. Арасланова
	подпись	дата	ФИО
		27.11.2020	Юрисконсульт Д.А. Босова
	подпись	Дата	ФИО

Лист ознакомления

№	Должность	ФИО	Подпись	Дата

Лист регистрации изменений

№ п/п	Номер изменения	Номер листа	Дата внесения изменения	Дата проверки	Лицо, внесшее изменения	
					ФИО	Подпись