МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ
Государственное бюджетное профессиональное образовательное учреждение
«БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНФОРМАЦИОННО—ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ» (ГБПОУ «БРИЭТ»)

СОГЛАСОВАНО
Педагогическим Советом
ГБПОУ «БРИЭТ»
протокол № 6
«27» января 2021г.

УТВЕРЖДАЮ
Директор ГБПОУ «БРИЭТ»
_____ Е.Д.Цыренов
Приказ № 19 от 27.01.2021

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГБПОУ «БРИЭТ»

КОНТРОЛЬНЫЙ ЭКЗЕМПЛЯР

г. Улан—Удэ
2021 г.

1. Общие положения

Положение об информационной безопасности в ГБПОУ «Бурятский республиканский информационно—экономический техникум» (далее — техникум), регламентирует порядок организации и правила обеспечения информационной безопасности, также распределение функций и ответственности за обеспечение информационной безопасности между сотрудниками техникума, требования по информационной безопасности к информационным средствам, применяемым в техникуме.

1.1. Правовую основу Положения составляют:

- Федеральный закон от 29.12.2012 г. № 273 ФЗ «Об образовании в Российской Федерации» (с изм. и доп.);

- Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ (с изм. и доп.);

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм и доп.);

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изм и доп.);

- Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (с изм. и доп.);

- другие законодательные акты, руководящие и нормативно-методические документы РФ в области обеспечения информационной безопасности

и имеет статус локального нормативного акта образовательной организации.

1.2. Под информационной безопасностью Техникума следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.3. Использование сети Интернет в образовательной организации подчинено следующим принципам:

- соответствие образовательным целям;

- способствование гармоничному формированию и развитию личности;

- уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;

-приобретение новых навыков и знаний;

- расширение применяемого спектра учебных и наглядных пособий;

- социализация личности, введение в информационное общество.

1.4. К объектам информационной безопасности в Техникуме относятся:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;

- информация, защита которой предусмотрена законодательными актами РФ, в т.ч. персональные данные;

- средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

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

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);

- целостность (точность и полноту информации и компьютерных программ);

- доступность (возможность получения пользователями информации в пределах их компетенции).

1.6. 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.

2. Правовые нормы обеспечения информационной безопасности

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

2.2. Техникум обязан обеспечить сохранность конфиденциальной информации.

2.3. Администрация школы:

- назначает ответственного за обеспечение информационной безопасности;

- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

- 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 техникума со стороны государственных и судебных инстанций.

2.4. Организационные и функциональные документы по обеспечению информационной безопасности:

- приказ директора Техникума 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 Техникума и др.

2.5. Порядок допуска сотрудников Техникума к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

- ознакомление работника с нормами законодательства РФ и Техникума 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. Использование сети Интернет

3.1. Использование сети Интернет в Техникуме осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.

3.2. Работники Техникума вправе:

- размещать информацию, касаемо преподаваемой дисциплины, в сети Интернет на интернет-ресурсах Техникума;

3.3. Работникам Техникума запрещено размещать в сети Интернет и на образовательных ресурсах информацию:

- противоречащую требованиям законодательства РФ и локальным нормативным актам Техникума;

- не относящуюся к образовательному процессу и не связанную с деятельностью Техникума;

- нарушающую нравственные и этические нормы, требования профессиональной этики.

3.4. Обучающиеся Техникума вправе:

- использовать ресурсы, размещенные в сети Интернет, в порядке и на условиях, которые предусмотрены настоящим Положением.

- размещать информацию и сведения на интернет-ресурсах Техникума, в частности, в системе дистанционного обучения Moodle.

5. Обучающемся запрещено:

- находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и / или нарушает законодательство РФ;

- осуществлять любые сделки через интернет;

- загружать файлы на компьютер Техникума без разрешения уполномоченного лица;

- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

6. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом директора Школы.

7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

7.1. Уполномоченное лицо обязано:

- принять сообщение пользователя;

- принять меры по отключению выхода на данный ресурс с интернет ресурсов Техникума;

- если обнаруженный ресурс явно нарушает законодательство РФ - сообщить о нем по специальной "горячей линии" для принятия мер в соответствии с законодательством РФ (в течение суток).

Передаваемая информация должна содержать:

- интернет-адрес (URL) ресурса;

- тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;

- дату и время обнаружения;

- информацию об установленных в образовательной организации технических средствах ограничения доступа к информации.

8. Мероприятия по обеспечению информационной безопасности

8.1. Для обеспечения информационной безопасности в Техникуме требуется проведение следующих первоочередных мероприятий:

- защита интеллектуальной собственности Техникума;

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

- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Техникума;

- учет всех носителей конфиденциальной информации.

9. Организация работы с информационными ресурсами и технологиями

9.1. Система организации делопроизводства:

- учет всей документации Техникума с классификацией по сфере применения, дате, содержанию;

- регистрация и учет всех входящих (исходящих) документов Техникума 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.

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

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

9.2.2. 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.

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

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

9.2.5. Запрещается выносить документы с грифом «Для служебного пользования» за пределы школы.

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

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

10. О системном администрировании и обязанностях ответственного за информационную безопасность

10.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы системного администратора.

10.2. Для решения задач информационной безопасности системный администратор обязан:

- следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);

- обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;

- обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;

- обеспечивать нормальное функционирование системы резервного копирования.

11. Антивирусная защита

11.1. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.). Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется посредством лицензионного антивирусного программного обеспечения.

11.2. За своевременное обновление антивирусного программного обеспечения отвечает системный администратор.

12. Установка и обслуживание оборудования, программ.

12.1. Установка и обслуживание оборудования возможна только сотрудниками Центра информационных технологий. Установка и обслуживание оборудования сотрудниками других отделов запрещена.

12.2. Установка программ возможна только сотрудниками Центра информационных технологий. Установка программ сотрудниками других отделов запрещена.

Разработчик: _____Очирова Н.В., методист

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Содержание изменения	Основание изменения	Дата изменения	Подпись лица, внесшего изменение

ЛИСТ СОГЛАСОВАНИЯ

№ пп	Должность	ФИО	Дата согласования	Подпись
1.	Заместитель директора	Аюшиева А.Б.	28.01.2021	
2.	Заведующий ЦИТ	Кулышев А.Л.	28.01.2021	
3.				
4.				