Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Нализко Наталья Александровна
Должность: Директор
Дата подписания: 30.09.2026 15:44:14
Уникальный программный ключ:
254679086555d9e0abdc452e51caba97c16aa1bcd

УТВЕРЖДЕНО
решением ученого совета филиала
«17» сентября 2026 г., пр. №01
Председатель ученого совета
_____ Н.А. Нализко

ПОЛОЖЕНИЕ

ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КИБЕРБЕЗОПАСНОСТИ) В КОСТАНАЙСКОМ ФИЛИАЛЕ ФГБОУ ВО «ЧЕЛЯБИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

П 126 - 2026

Костанай, 2026

Запрещается несанкционированное копирование документа

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН – Альжановой З.А., начальником отдела оценки качества образования

2 ВВЕДЕН В ДЕЙСТВИЕ приказом директора филиала от «25» сентября 2026 г. №126/04-06

3 ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 1 год

4 ВВЕДЕН ВПЕРВЫЕ 2026

Настоящее Положение не может быть полностью или частично воспроизведено, тиражировано и распространено в качестве официального издания без разрешения директора Костанайского филиала ФГБОУ ВО «ЧелГУ»

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Положение об обеспечении информационной безопасности (кибербезопасности) в Костанайском филиале ФГБОУ ВО «Челябинский государственный университет» (далее – Положение) определяет основные цели, задачи, принципы, требования и порядок организации мероприятий по защите информационных ресурсов, информационных систем, цифровых объектов и данных в Костанайском филиале федерального государственного бюджетного образовательного учреждения высшего образования «Челябинский государственный университет» (далее – филиал).

1.2 Информационная безопасность в филиале направлена на обеспечение кибербезопасности, включающей в себя надежные пароли и двухфакторную аутентификацию, ограничение доступа работников к информации, защиту персональных данных, антивирусную защиту, резервное копирование, правила использования электронной почты и мессенджеров, порядок действий при взломе или утечке данных.

1.3 Настоящее Положение распространяется на работников филиала, обучающихся, а также иных лиц, имеющих доступ к информационным системам, информационным ресурсам, цифровым объектам, компьютерному оборудованию и сетевой инфраструктуре филиала.

2 НОРМАТИВНЫЕ ССЫЛКИ

Настоящее Положение разработано с учетом требований и принципов, изложенных в следующих нормативных документах:

2.1 Федеральный закон от 27 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

2.2 Цифровой кодекс Республики Казахстан от 09 января 2026 года № 255-VIII.

2.3 Трудовой кодекс Республики Казахстан от 23 ноября 2015 года № 414-V.

2.4 Закон Республики Казахстан «О кибербезопасности» от 24 ноября 2015 года № 418-V ЗРК (в действующей редакции).

2.5 Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины, используемые в настоящем Положении:

Информационная безопасность	состояние защищенности информационных ресурсов, информационных систем, цифровых объектов и данных от неправомерного доступа, использования, изменения, распространения, уничтожения и иных угроз.
Кибербезопасность	состояние защищенности цифровых объектов и деятельности, связанной с их функционированием, от киберугроз и неправомерного воздействия.
Кибергигиена	совокупность повседневных правил и практических действий пользователя, направленных на безопасное использование информационных систем, цифровых устройств, информационных ресурсов и сети Интернет, а также на

Запрещается несанкционированное копирование документа

	предупреждение киберугроз.
Цифровой объект	информационная система, информационный ресурс, программно-технический комплекс и иные цифровые объекты, используемые филиалом.
Информационная система	совокупность информационно-коммуникационных технологий, информационных ресурсов и иных средств, предназначенных для решения определенных задач.
Информационный ресурс	сведения и данные, хранящиеся, обрабатываемые или передаваемые посредством информационных систем.
Персональные данные	сведения или совокупность сведений о субъекте персональных данных, дополненные одним или несколькими идентификаторами персональных данных
Учетная запись	совокупность идентификационных данных пользователя, предназначенная для его идентификации и предоставления ему определенных прав доступа.
Аутентификация	процедура проверки принадлежности пользователю предъявленного им идентификатора.
Инцидент информационной безопасности	событие или совокупность событий, которые привели или могут привести к нарушению конфиденциальности, целостности или доступности информации, информационных ресурсов или информационных систем.
Резервное копирование	создание копий данных для обеспечения возможности их восстановления в случае утраты, повреждения или уничтожения
Пользователь	работник, обучающийся или иное лицо, которому предоставлен доступ к информационным системам или ресурсам филиала.

4 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Филиал	Костанайский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Челябинский государственный университет».
РК	Республика Казахстан

5 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КИБЕРБЕЗОПАСНОСТИ)

5.1 Основной целью обеспечения информационной безопасности (кибербезопасности) филиала является обеспечение защищенности информационных систем, цифровых ресурсов и данных филиала, а также формирование у работников и обучающихся навыков безопасного поведения в цифровой среде.

5.2 Основными задачами являются:

- обеспечение конфиденциальности, целостности и достоверности информации;
- реализация защиты всех информационных ресурсов от несанкционированного доступа и повреждений;
- предупреждение компьютерных атак и иных киберугроз;
- предотвращение, выявление и устранение уязвимостей, утечек и потерь;

Запрещается несанкционированное копирование документа

- обеспечение безопасного использования информационных систем;
- сохранение конфиденциальности данных филиала, включая персональные данные работников и обучающихся;
- обеспечение резервного копирования и восстановления данных;
- своевременное выявление и реагирование на инциденты информационной безопасности;
- повышение уровня осведомленности работников и обучающихся в области информационной безопасности;
- обеспечение соблюдения требований законодательства Республики Казахстан (далее – РК) и локальных нормативных актов филиала.

6 ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КИБЕРБЕЗОПАСНОСТИ)

6.1 Обеспечение информационной безопасности (кибербезопасности) осуществляется на основе следующих принципов:
- законность – сбор, обработка и хранение информации строятся строго в рамках действующего законодательства;
- конфиденциальность – доступ к секретным данным имеют только уполномоченные лица;
- целостность – данные остаются точными, полными и защищенными от случайных или намеренных изменений;
- доступность – авторизованные пользователи могут получить нужные файлы и системы в любой момент, когда это необходимо;
- контролируемость – все действия с документами и базами данных фиксируются, что позволяет узнать, кто и когда вносил изменения.

7 ОРГАНИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КИБЕРБЕЗОПАСНОСТИ)

7.1 Общее руководство организацией мероприятий по обеспечению информационной безопасности (кибербезопасности) осуществляет руководство филиала.
7.2 Руководство Филиала:
- определяет перечень необходимых локальных документы в сфере информационной безопасности (кибербезопасности);
- определяет ответственных лиц;
- обеспечивает организацию необходимых мероприятий по защите информации;
- обеспечивает условия для обучения работников;
- обеспечивает принятие мер по предупреждению и устранению последствий инцидентов;
- осуществляет общий контроль соблюдения требований настоящего Положения.

7.3 Ответственное лицо или структурное подразделение по информационной безопасности (кибербезопасности):
- координирует мероприятия по информационной безопасности (кибербезопасности);
- организует информирование работников;
- участвует в проведении обучения;

Запрещается несанкционированное копирование документа

- осуществляет мониторинг соблюдения установленных требований;
- организует регистрацию и анализ инцидентов;
- участвует в подготовке предложений по совершенствованию системы защиты.

7.4 Работники и обучающиеся филиала обязаны:

- соблюдать требования законодательства РК в сфере информационной безопасности, кибербезопасности и защиты персональных данных;
- соблюдать настоящее Положение и иные локальные документы филиала;
- соблюдать правила кибергигиены;
- обеспечивать конфиденциальность своих учетных данных;
- использовать предоставленные права доступа исключительно в служебных и учебных целях;
- не передавать другим лицам логины, пароли, коды подтверждения и иные средства аутентификации;
- не устанавливать несанкционированное программное обеспечение;
- соблюдать правила работы с электронной почтой и сетью Интернет;
- обеспечивать сохранность служебной информации;
- соблюдать требования по защите персональных данных;
- незамедлительно сообщать о выявленных подозрительных действиях, нарушениях или инцидентах;
- проходить предусмотренное обучение и инструктажи.

7.5 Работник не вправе ссылаться на незнание требований информационной безопасности после прохождения установленного порядка ознакомления с соответствующими документами.

7.6 Работники и обучающиеся обязаны соблюдать установленные требования информационной безопасности (кибербезопасности) и незамедлительно сообщать о выявленных угрозах и инцидентах.

8 УПРАВЛЕНИЕ ДОСТУПОМ

8.1 Доступ к информационным системам предоставляется пользователю в объеме, необходимом для выполнения его должностных или учебных обязанностей.

8.2 Каждый пользователь должен использовать персональную учетную запись, если иное не предусмотрено особенностями функционирования конкретной информационной системы.

8.3 Запрещается:

- передавать логин и пароль другим лицам;
- использовать чужие учетные записи;
- предоставлять доступ к информационной системе филиала лицам, не имеющим соответствующих полномочий;
- использовать учетную запись другого работника или обучающегося;
- обходить установленные механизмы защиты.

8.4 При переводе работника, изменении его должностных обязанностей или прекращении трудовых отношений права доступа подлежат пересмотру или прекращению.

8.5 При прекращении трудовых или иных отношений доступ пользователя к информационным системам подлежит своевременному прекращению.

Запрещается несанкционированное копирование документа

9 ТРЕБОВАНИЯ К ПАРОЛЯМ И АУТЕНТИФИКАЦИИ

9.1 Каждый пользователь обязан обеспечивать конфиденциальность своих паролей и иных средств аутентификации.
9.2 Пароли должны быть сложными, индивидуальными и не использоваться одновременно для различных информационных систем, если технические возможности позволяют обеспечить такое требование.
9.3 Не допускается использование в качестве паролей очевидных комбинаций, включая имя пользователя, дату рождения, номер телефона, название подразделения и иные легко угадываемые сведения.
9.4 При подозрении на компрометацию учетной записи пользователь обязан незамедлительно изменить пароль и сообщить об инциденте ответственному лицу.
9.5 При наличии технической возможности филиал применяет дополнительные средства аутентификации.

10 БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ И РЕСУРСОВ СЕТИ ИНТЕРНЕТ

10.1 Доступ к локально-вычислительной сети филиала, электронному документообороту и сети Интернет предоставляются и используются для выполнения служебных и образовательных задач.
10.2 При использовании электронной почты работник обязан проверять:
- адрес отправителя;
- содержание сообщения;
- наличие подозрительных вложений;
- адреса ссылок;
- наличие требований предоставить пароль, код или иные конфиденциальные сведения.

10.3 При получении подозрительного письма работник не должен переходить по содержащимся в нем ссылкам или открывать вложения.
10.4 При использовании сети Интернет запрещается:
- осуществлять попытки несанкционированного доступа к информационным системам;
- распространять вредоносное программное обеспечение;
- осуществлять действия, направленные на нарушение работы информационных систем;
- использовать ресурсы филиала для противоправной деятельности;
- устанавливать программное обеспечение без соответствующего разрешения.

10.5 При возникновении сомнений работник обязан обратиться к ответственному лицу.

11 МОБИЛЬНЫЕ УСТРОЙСТВА И СЪЕМНЫЕ НОСИТЕЛИ

11.1 Использование мобильных устройств для доступа к информационным системам филиала допускается при соблюдении установленных требований безопасности.
11.2 Устройства должны быть защищены паролем, PIN-кодом, биометрической аутентификацией или иным предусмотренным средством защиты.
11.3 При утрате мобильного устройства, имеющего доступ к информационным системам филиала, работник обязан незамедлительно сообщить об этом ответственному лицу.
11.4 Использование USB-накопителей и иных съемных носителей допускается при наличии

Запрещается несанкционированное копирование документа

служебной или учебной необходимости.
11.5 Перед использованием съемные носители должны проверяться на наличие вредоносного программного обеспечения.
11.6 Запрещается использовать неизвестные или обнаруженные носители информации без предварительной проверки.
11.7 Запрещается копировать на съемные носители персональные данные и иную информацию ограниченного доступа без соответствующего основания и необходимости.

12 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

12.1 Филиал обеспечивает резервное копирование критически важных данных.
12.2 Порядок резервного копирования определяется ответственным подразделением или лицом с учетом особенностей конкретной информационной системы.
12.3 Резервные копии должны быть защищены от несанкционированного доступа и уничтожения.
12.4 Периодически проводится проверка возможности восстановления данных из резервных копий.

13 ВЫЯВЛЕНИЕ И РЕАГИРОВАНИЕ НА КИБЕРИНЦИДЕНТЫ

13.1 К киберинцидентам относятся:
- заражение компьютера вредоносным программным обеспечением;
- несанкционированный доступ;
- компрометация учетной записи;
- утечка или незаконное распространение данных;
- потеря оборудования;
- несанкционированное изменение данных;
- нарушение доступности информационной системы;
- фишинговые атаки;
- подозрение на компьютерную атаку;
- иные события, способные нарушить информационную безопасность (кибербезопасностиь).

13.2 Пользователь обязан незамедлительно сообщить ответственному лицу, если:
- обнаружил подозрительное письмо;
- открыл подозрительную ссылку;
- обнаружил неизвестную программу;
- заметил необычную работу компьютера;
- потерял устройство;
- обнаружил попытку входа в свою учетную запись;
- ошибочно направил информацию не тому адресату;
- обнаружил факт или подозрение на утечку информации;
- выявил иное нарушение безопасности.

13.3 При обнаружении инцидента пользователь обязан:
- прекратить действия, которые могут усугубить последствия инцидента;
- по возможности сохранить информацию об инциденте;
- незамедлительно сообщить ответственному лицу;

Запрещается несанкционированное копирование документа

- выполнять указания ответственных специалистов;
- самостоятельно удалять следы инцидента, если это может препятствовать его расследованию.

13.4 Ответственное лицо организует регистрацию, анализ и устранение последствий инцидента. Форма журнала закреплена в приложении А.

13.5 При необходимости филиал осуществляет взаимодействие с поставщиками информационных систем и иными уполномоченными организациями в соответствии с законодательством и установленными процедурами.

14 ОБУЧЕНИЕ И КИБЕРГИГИЕНА РАБОТНИКОВ

14.1 Филиал организует обучение и повышение осведомленности работников в сфере информационной безопасности, кибербезопасности и кибергигиены.

14.2 Обучение может включать:
- вводный инструктаж;
- периодические инструктажи;
- тематические занятия;
- практические тренинги;
- информирование о новых видах киберугроз;
- обучение безопасной работе с электронной почтой;
- обучение правилам работы с персональными данными;
- обучение действиям при возникновении инцидентов;
- проверку знаний и практических навыков.

14.3 Особое внимание при обучении уделяется:
- фишингу;
- социальной инженерии;
- вредоносному программному обеспечению;
- защите паролей;
- безопасному использованию электронной почты;
- защите персональных данных;
- безопасному использованию мобильных устройств;
- безопасному использованию сети Интернет;
- действиям при инцидентах.

14.4 Для отдельных категорий работников, имеющих специальные полномочия или доступ к критически важным информационным системам, проводится дополнительное обучение в соответствии с установленными требованиями.

15 ПОРЯДОК ОЗНАКОМЛЕНИЯ РАБОТНИКОВ И ОБУЧАЮЩИХСЯ С ТРЕБОВАНИЯМИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КИБЕРБЕЗОПАСНОСТИ)

15.1 Работники и обучающиеся филиала подлежат ознакомлению с:
- настоящим Положением;
- правилами кибергигиены;
- инструкциями по работе с информационными системами;
- требованиями по защите персональных данных;

Запрещается несанкционированное копирование документа

- иными локальными документами в области информационной безопасности (кибербезопасности), применимыми к их деятельности.

15.2 Ознакомление осуществляется:

- до предоставления соответствующего доступа к информационным системам – в необходимых случаях;
- при внесении существенных изменений в документы;
- при введении новых информационных систем или технологий;
- в иных случаях, установленных филиалом.

15.3 Факт ознакомления подтверждается подписью работника (обучающегося) либо иным способом, позволяющим достоверно установить факт ознакомления.

15.4 Ознакомление работника филиала с настоящим Положением означает подтверждение факта получения информации о предъявляемых требованиях и обязанности их соблюдать.

15.5 Ознакомление с настоящим Положением не является согласием на обработку персональных данных.

15.6 Согласие на сбор, обработку, распространение или передачу персональных данных оформляется отдельно в случаях и порядке, предусмотренных законодательством РК.

16 КОНТРОЛЬ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (КИБЕРБЕЗОПАСНОСТИ)

16.1 Контроль осуществляется руководством филиала и назначенными ответственными лицами.

16.2 Контроль может включать:

- проверку соблюдения прав доступа;
- проверку выполнения требований к защите персональных данных;
- анализ инцидентов;
- проверку прохождения обучения;
- контроль ознакомления работников с документами;
- оценку уровня кибергигиены;
- иные мероприятия.

17 ОТВЕТСТВЕННОСТЬ

17.1 Лица, нарушившие требования настоящего Положения, несут ответственность в соответствии с законодательством РК.

17.2 К нарушениям относятся:

- передача учетных данных;
- использование чужой учетной записи;
- разглашение конфиденциальной информации;
- неправомерное распространение персональных данных;
- установка неразрешенного программного обеспечения;
- нарушение правил работы с информационными системами;
- сокрытие выявленного инцидента;
- умышленное нарушение функционирования информационных систем;
- иные нарушения требований информационной безопасности (кибербезопасности).

Запрещается несанкционированное копирование документа

18 ИЗМЕНЕНИЯ

18.1 Положение вступает в силу с момента введения его в действие приказом директора филиала.
18.2 Возможные изменения и дополнения согласуются и утверждаются в установленном порядке.
18.3 Ответственность за своевременное внесение дополнений и изменений в положение несет начальник отдела оценки качества образования.

19 СОГЛАСОВАНИЕ, ХРАНЕНИЕ И РАССЫЛКА

19.1 Проект положения согласовывается с:
– директором филиала;
– заместителем директора по учебной работе;
– заместителем директора по научной работе;
– начальником информационно-технического отдела;
– начальником отдела кадров.
19.2 Рассылка учтенных рабочих экземпляров положения должна осуществляться отделом оценки качества образования в структурные подразделения.
19.3 Ответственность за хранение учтенного рабочего экземпляра положения несет отдел оценки качества образования.

Запрещается несанкционированное копирование документа

Приложение А
(обязательное)

Форма журнала регистрации инцидентов информационной безопасности

№	Дата и время	Описание инцидента	Информационная система/ресурс	Принятые меры	Ответственное лицо	Дата закрытия

Запрещается несанкционированное копирование документа

Приложение Б
(обязательное)

Лист согласования

Должность	ФИО	Дата	Подпись
1	2	3	4
Директор филиала	Нализко Н.А.		
Заместитель директора по учебной работе	Панина Г.В.		
Заместитель директора по научной работе	Нурмагамбетов Р.Г.		
Начальник информационно-технического отдела	Ефимов И.А.		
Начальник отдела кадров	Мартынец М.А.		

Запрещается несанкционированное копирование документа

Приложение В
(обязательное)

Лист ознакомления

Должность	ФИО	Дата	Подпись
1	2	3	4

Приложение Г
(обязательное)

Лист регистрации изменений

Номер изменения	Номер извещения об изменении	Номер листов (страниц)				Всего листов (после изменений)	Дата внесения изменения	Ф.И.О. осуществляющего внесение изменений	Подпись лица вносившего изменения
		измененных	замененных	новых	аннулированных				
1	2	3	4	5	6	7	8	9	10

Приложение Д
(обязательное)

Лист учета периодических проверок

Дата проверки	ФИО лица, выполнившего проверку	Подпись лица, выполнившего проверку	Формулировка замечаний
1	2	3	4