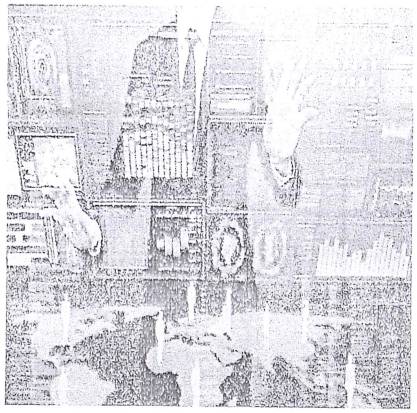


Утверждено приказом
директора филиала
от "25" 09 2026 № 1021/1-Х

ПОЛОЖЕНИЕ
о системе управления информационной безопасностью Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации»

1. Общие положения

1.1. Целью настоящего Положения является определение основных требований, обязательных для исполнения работниками при работе с компьютеризированными системами в Минском филиале УО «Белорусский торгово-экономический университет потребительской кооперации».

1.2. Положение распространяется на выполнение любых работ посредством персонального компьютера (далее – ПК).

1.3. Ответственность за ознакомление с Положением несет заведующий сектором информационных технологий Хайков В.П.

1.4. Контроль за исполнением требований настоящего Положения возлагается на сектор информационных технологий Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации».

1.5. Ответственность по обеспечению технической информационной безопасности возлагается на администратора, в случае отсутствия администратора на заведующего сектора информационных технологий Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации».

2. Используемые термины и определения:

Информационная безопасность (далее - ИБ) представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов от угроз информационной безопасности. Меры защиты программно-технического уровня реализуются при помощи соответствующих программно-технических средств и методов защиты информации.

Информационная система (далее - ИС) - представляет собой совокупность объектов, информационный обмен между которыми осуществляется посредством локальной-вычислительной сети и/или использования открытых каналов связи, предоставленных сторонними операторами электросвязи.

Программное обеспечение (далее - ПО) - это совокупность всех программ и соответствующей документации, обеспечивающая использование компьютера в интересах его пользователя.

Персональный компьютер (далее - ПК) - электронная вычислительная машина, предназначенная для обеспечения деятельности одного пользователя.

Администратор – сотрудник сектора информационных технологий Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации», должностные обязанности которого включает обеспечение штатной работы парка компьютерной техники, локальной сети и программного обеспечения Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации», в том числе обеспечение информационной безопасности в организации.

Пользователь - должностное лицо, исполнение должностных обязанностей которого систематически или эпизодически связано с работой на персональном компьютере.

Лицензиар – правообладатель программного обеспечения;

Локальная сеть, компьютерная сеть (вычислительная сеть, сеть передачи данных) (далее - сеть) – система связи двух или более компьютеров и/или компьютерного оборудования (серверы, маршрутизаторы и другое оборудование).

База данных (далее - БД) — совместно используемый набор логически связанных данных (и описание этих данных), предназначенный для удовлетворения информационных потребностей организации, в т.ч. данные программ бухгалтерского учета и программ в которых ведется учет товародвижения.

Электронная почта – учетная запись на почтовом сервере Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации» в домене mtk-bks.by.

3. Требования к ПК в организации

ПК в организации (на предприятии) (далее – организации) должны удовлетворять следующим требованиям:

смена пароля пользователя на доступ к ПК должна производиться не реже одного раза в год, для администраторов организаций - не реже одного раза в полгода. Пароль должен удовлетворять требованиям сложности;

изменение предъявляемых требований к отдельным ПК принимается сектором информационных технологий на основании мотивированного ходатайства руководителя структурного подразделения (отделения) Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации». Перечень данных ПК хранится в секторе информационных технологий и/или администратора.

4. Порядок предоставления прав доступа к компьютерной технике, ресурсам и программам локально-вычислительной сети организации

4.1. Подключение пользователей к информационной системе, а также предоставление доступа к базам данных производится только администратором

с обязательным присвоением каждому пользователю логического имени («логина») и пароля, либо группового логина (для отдела, сектора и т.д.) с единым паролем. Групповой логин и пароль может применяться только в случаях выполнения аналитической работы с базой данных без внесения изменений и дополнений.

4.2. Права учетной записи пользователей должны быть достаточными для выполнения ими своих служебных обязанностей.

4.3. Администратором предоставляется право доступа Лицензиарам, правообладателям к их программному обеспечению, для выполнения договорных условий по его обновлению. При этом администратором выполняются требования, установленные в соответствии с заключенным договором между Лицензиаром и/или правообладателем и организацией. Доступ Лицензиару предоставляется разовый, имеет сменный пароль при каждом последующем подключении, на основании запроса Лицензиара и/или работника организации. В запросе и/или служебной записке отражается наименование программы, наименование правообладателя, компании, осуществляющей работы над программным обеспечением, причина предоставления доступа, временной период, на который необходимо предоставить доступ, IP адрес, с которого необходим доступ.

4.4. Постоянный доступ работникам организации к сети Интернет и личным почтовым ящикам предоставляется администратором при потребности в рамках функциональных обязанностей.

5. Работа с сетевыми ресурсами

5.1. На персональных компьютерах специалистов не должно быть локальных дисков со статусом «Общий доступ».

5.2. Для временного хранения файлов, а также для обмена информацией между структурными подразделениями в Минском филиале УО «Белорусский торгово-экономический университет потребительской кооперации» возможно использование сетевого ресурса «Внутренний документооборот» (\\192.168.1.200\Внутренний документооборот). Данный сетевой раздел предназначен только для кратковременного хранения информации.

5.3. Для эффективной работы с электронной почтой входящая и исходящая корреспонденция, срок хранения которой превышает 2 года должна удалятся. Очистка невостребованной корреспонденции должна проводится в последние числа каждого месяца.

5.4. **Использование сети интернет только в служебных целях.**

6. Права и обязанности пользователей и администраторов

6.1. Администратор обязан:

производить регламентированный доступ сотрудников к ресурсам локальной вычислительной сети, в том числе ресурсам сети Интернет;

контролировать статистику использования ресурсов сети Интернет пользователями;

контролировать уязвимости информационной системы к вирусным атакам;

обеспечивать все компьютеры антивирусным программным обеспечением, а также систематическое обновление антивирусных баз данных;

поддерживать регламентированную работу пользователей сети при использовании электронной почты, удаленного доступа через защищенные каналы передачи данных;

осуществлять блокировку неконтролируемого обмена информацией между рабочими местами пользователей;

контролировать активность, связанную с доступом и использованием средств антивирусной защиты;

осуществлять мониторинг событий, связанных с информационной безопасностью;

участвовать в действиях по восстановлению работоспособности сети после сбоев и аварий;

6.2. Администратор имеет право:

выбирать технические и программные средства управления и обеспечения ИБ, и вносить предложения по их приобретению, в соответствии с порядком, установленным локальными документами Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации»;

вносить предложения по изменению политики информационной безопасности;

контролировать выполнение установленных правил создания, хранения и использования программных средств, соблюдение порядка формирования и использования информационных массивов и баз данных, резервного и архивного копирования данных;

6.3. Права и обязанности пользователей:

принимать участие в технических совещаниях при обсуждении вопросов использования программного обеспечения или предоставления доступа к информационным ресурсам;

вносить предложения по использованию ПК для более эффективного выполнения должностных обязанностей;

использовать ресурсы и сервисы, предоставляемые сетью, к которым у него открыт доступ (общие папки на ПК и серверах, принтеры, предоставленные в совместный доступ по сети, базы данных и т.п.);

создавать собственные информационные ресурсы (размещение материалов в своей папке или общем сетевом каталоге на сервере), доступные всем или выборочным пользователям сети;

представлять в сектор информационных технологий, администратору предложения по созданию новых ресурсов, сервисов, узлов сети с целью улучшения ее работы и расширения ее возможностей.

6.4. Пользователь обязан:

выполнять требования администратора, связанные с настройкой сетевого программного обеспечения, установкой дополнительных обновлений для операционных систем и необходимых обновлений антивирусных пакетов на подключенном к сети компьютере;

не разглашать свои пароли (пароли для доступа в сеть, к электронной почте и т.п.). Пользователь самостоятельно осуществляет смену пароля. В

случае если пароль утерян или стал известен другому пользователю, производится немедленная его смена. В случае увольнения сотрудника, администратором производится блокирование его учетной записи сроком до 1 года с последующим ее удалением, либо смена пароля руководителем структурного подразделения при использовании группового логина;

обеспечивать сохранность информации, распространение и (или) предоставление которой ограничено;

сообщать администратору о проблемах или перебоях в работе сети и компьютерного оборудования;

в целях обеспечения защиты информации пользователь обязан:

создавать резервные копии важной информация на сменных носителях или по согласованию с администратором организации на специально отведенном диске сервера;

обеспечить сохранность конфиденциальных данных, содержащихся как на ПК, так и на сменных носителях;

проверять на наличие вирусов все носители информации, получаемые или передаваемые;

6.5. Пользователю запрещается:

самостоятельно ремонтировать и производить техническое обслуживание вычислительной техники;

использовать интернет-протоколы и программы, публичные системы мгновенных сообщений (Skype, Viber и др.), а также посещение социальных сетей («Одноклассники», «Вконтакте» и др.), за исключением категорий работников в чьи обязанности входит использование данных приложений;

использовать пиринговые (P2P) сетевые сервисы для обмена файлами через Интернет, такие как Torrent, Emule и др.

самостоятельно устанавливать и удалять какие-либо программы на свой ПК, установка дополнительного ПО осуществляется по запросу и при наличии технической возможности;

самостоятельно подключать к компьютеру и отключать какие-либо устройства, в том числе любые внешние источники подключения к сети Интернет;

совершать действия, создающие помехи в работе другим пользователям сети;

самостоятельно изменять сетевые настойки ПК или настройки общего доступа к общим ресурсам;

использовать компоненты программного и аппаратного обеспечения в неслужебных целях;

посещать интернет-сайты содержащие информацию, экстремистской, порнографической направленности, сайты социальных сетей;

получать и отправлять по электронной почте программное обеспечение без согласования с администратором организации;

предоставлять посторонним лицам физический или удаленный доступ к своему компьютеру;

предоставлять права удаленного доступа к системным ресурсам своего ПК (корневой раздел жесткого диска, на котором установлена операционная система, каталоги, в которых установлена операционная система);

оставлять включенный без присмотра свой ПК, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

использовать аппаратные и программные средства, которые могут нанести физический ущерб или уничтожить данные, хранящиеся на серверах сети или компьютерах других пользователей;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению конфликтной ситуации. Об обнаружении такого рода ошибок ставить в известность администратора и руководителя своего структурного подразделения организации;

блокировать доступ к ресурсам сети или компьютерам пользователей;

хранить и использовать на своем ПК материалы, не относящиеся к исполнению служебных обязанностей;

записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации;

предпринимать попытки взлома компьютерной защиты ПК других пользователей, сети организации, ресурсов сторонних организаций;

предпринимать действия, направленные на несанкционированное получение прав доступа к программам, базам данных и иной информации, хранящейся в сети, на ПК других пользователей;

сообщать, кому бы то ни было, кроме непосредственного руководителя в случае режима замещения, свой пароль;

посылать в электронном виде информацию, содержащую сведения ограниченного распространения без применения программного обеспечения для ее защиты;

получать и использовать несанкционированный удалённый доступ на управление ПК других пользователей и серверов, а также предоставлять закреплённый за ними ПК в пользование другим лицам, в том числе для удаленного доступа;

отключать свой ПК от сети;

распространять по электронной почте, либо другими способами с использованием сети, любую информацию или материалы, классифицируемые как спам, порнографические материалы, материалы экстремистского, террористического плана и т.п. в соответствии с законодательством Республики Беларусь.

7. Контроль за соблюдением требований по обеспечению информационной безопасности

Использование Пользователями ПК, доступа в Интернет и электронной почты может наблюдаться, протоколироваться и периодически проверяться, в том числе по запросу руководителя структурного подразделения.

Ответственными должностными лицами за реализацию порядка обеспечения информационной безопасности в сети являются администратор, руководители структурных подразделений Минского филиала УО «Белорусский торгово-экономический университет потребительской

кооперации», отвечающие непосредственно за работу своих подчиненных с предоставленными ресурсами сети Интернет в соответствии с возложенными на них должностными обязанностями и поручениями.

7.1. Для определения эффективности использования подчиненными пользователями ресурсов сети Интернет, руководитель структурного подразделения Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации» обязан:

периодически контролировать доступ своих подчиненных в сеть Интернет;

доводить до руководителя или курирующего заместителя факты использования сети Интернет в неслужебных целях.

7.2. Разграничение ответственности по информационной безопасности:

ответственность за безопасность загруженной информации через Интернет и электронную почту, возлагается на пользователя осуществившего приём этой информации.

ответственность за информационную безопасность при работе в сети организации, установку и обновление сетевого антивирусного программного обеспечения, своевременную установку программных систем возлагается на администратора, что фиксируется в должностной инструкции.

В целях проведения проверок устойчивости компьютерной защиты, соблюдения Пользователями требований настоящего Положения ответственными сотрудниками сектора информационных технологий могут проводиться проверочные мероприятия, не нарушающие целостность и работоспособность аппаратно-программных средств.

8. Порядок применения средств антивирусной защиты информации

Антивирусная защита является обязательным программным продуктом, устанавливаемым на все ПК Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации», с целью предотвращения проникновения в систему компьютерных вирусов.

Программа антивирусной защиты для установки на объекты информатизации выбирается администратором организации с учетом количества информационных систем и обрабатываемой информации.

Антивирусные базы обновляются автоматически по мере появления обновления.

Ответственность за обновление базы несёт администратор.

Ответственность за функционирование программы антивирусной защиты возложена на администраторов.

Контроль за функционированием программы антивирусной защиты осуществляет администратор.

9. Порядок действий при возникновении несанкционированного доступа к информационным ресурсам

К попыткам несанкционированного доступа относятся:

сеансы работы незарегистрированных пользователей, или пользователей, *нарушивших установленную периодичность доступа, или срок действия*

полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

действия третьего лица, пытающегося получить доступ (или уже получившего доступ), при использовании учётной записи администратора или другого пользователя, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

При выявлении факта несанкционированного доступа администратор обязан:

прекратить несанкционированный доступ;

доложить непосредственному руководителю служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

известить руководителя структурного подразделения организации, в котором работает пользователь, о факте несанкционированного доступа.

В случае проблем при работе с Интернет, электронной почтой обращаться к администратору.

10. Работа с электронно-цифровыми ключами

Должностное лицо которое по роду своей деятельности использует электронно-цифровой ключ обязано:

обеспечить конфиденциальность данных личного ключа;

обеспечивать защиту личного ключа от случайного уничтожения или модификации (изменения);

не использовать личный ключ, если соответствующий ему открытый ключ отозван или срок действия этого открытого ключа истек;

отозвать открытый ключ в случае, если конфиденциальность соответствующего ему личного ключа нарушена.

11. Резервирование и уничтожение информации

Резервное копирование информационных ресурсов, является обязательным мероприятием по обеспечению сохранности и сохранению целостности информации.

Резервному копированию подлежат все базы данных, а также информация особо важная для работы.

Резервное копирование баз данных осуществляется ежедневно.

Ответственность за выполнение резервного копирования баз данных возложена на администратора.

Базы данных программ бухгалтерского учета, кадрового учета и иных автоматизированных систем должны копироваться и храниться на выделенном защищенном носителе. Актуализация баз данных должна осуществляться не реже одного раза в день. Выделенный защищенный носитель не должен храниться в помещении, в котором установлен сервер.

Администратор контролирует удаление неактуальной корреспонденции на ПК пользователем при достижении выделенной квоты на почтовом сервере.

Осуществляет системную настройку процесса удаления информации на ПК пользователей. Не должно быть настроек позволяющих удалять информацию минуя системную паку «Корзина».

12. Резервное питание

Обязательно осуществление резервного питания всех серверов Минского филиала УО «Белорусский торгово-экономический университет потребительской кооперации».

При сбое питания технические средства резервирования питания должны обеспечивать время достаточное для нормального завершения работы выполняемых программ и нормального режима завершения работы серверов.

Контроль за функционированием технических средств резервирования питания осуществляет администратор.

13. Ответственность

За неисполнение требований по информационной безопасности руководители управлений, отделов, секторов и пользователи несут ответственность в соответствии с законодательством Республики Беларусь.

Заведующий сектором
информационных технологий В.П. Хайков