МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«БРЯНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА И.Г. ПЕТРОВСКОГО»
(БГУ)

УТВЕРЖДАЮ
Ректор Брянского
государственного университета
имени академика И.Г.Петровского

_____ А.В. Антюхов

«__» _____ 2022 г.

ИНСТРУКЦИЯ
по правилам работы сотрудников университета в сети Интернет

1. Общие положения

1.1. Целями инструкции по правилам работы сотрудников (далее Инструкция) являются создание организационной и нормативно-правовой основы регулирования информационных процессов в корпоративной информационной сети (далее КИС) ФГБОУ ВО «Брянский государственный университет имени академика И.Г. Петровского» (далее – Университет), организация совместной работы администраторов КИС, индивидуальных Абонентов и коллективных пользователей сети.

1.2. Инструкция призвана обеспечить надежную и эффективную работу корпоративной информационной сети и каналов, обеспечивающих доступ к глобальной информационно-телекоммуникационной сети Интернет (далее – Интернет), сервисам электронной информационно-образовательной среды университета (далее ЭИОС).

2. Работа в сети Интернет

2.1. Разрешается работа в сети Интернет только через почтовые и прокси-сервера университета.

2.2. Передача электронной информации внутри и между подразделениями осуществляется исключительно через корпоративную почту на домене brgu.ru или внутри корпоративного портала, расположенных внутри КИС.

2.3. Устанавливаются следующие ограничения на получение информации из сети Интернет с доступом через сеть Университета:

запрещается работа в сети Интернет для неавторизованных сотрудников;

запрещается использование сети Интернет в личных коммерческих целях, не связанных с осуществлением трудовой деятельности;

по всем каналам связи по решению оператора КИС может накладываться ограничение на получение файлов звуковых и видео-форматов;

на все каналы связи по решению оператора КИС может накладываться ограничение на размер получаемого файла до 100 Мбайт;

запрещается передача информации, запрещенной действующим законодательством и локальными нормативными актами университета.

2.3. Изменение ограничений рассматривается по личным заявкам руководителей структурных подразделений с указанием причины и ресурса сети Интернет, с которого необходимо производить получение информации. Заявки рассматриваются в индивидуальном порядке и могут быть отклонены.

3. Часы работы в КИС и Интернет

3.1. Выход в сеть Интернет разрешен в период с 7:00 до 23:00. В ночное время с 23:00 до 7:00 выход в сеть Интернет запрещен для всех сотрудников, за исключением особых случаев, с разрешения руководства университета.

3.2. Работа в ночное время разрешается для отдельных серверов и рабочих станций, список которых должен быть согласован с руководством университета и отделом компьютерных технологий с указанием причины необходимости ночного доступа. При отсутствии утвержденного списка работа в ночное время запрещена.

4. Правила работы пользователей в сети Интернет

4.1. При пользовании сервисами сети Интернет пользователям необходимо строго соблюдать следующие требования безопасности:

4.1.1. При работе на автоматизированном рабочем месте с доступом в сеть Интернет (персональный компьютер, ноутбук и т.д.):

регулярно (не реже 1 раз в 6 месяцев) менять пароли доступа к автоматизированному рабочему месту и его сервисам;

убедиться, что средство антивирусной защиты активировано и корректно работает;

убедиться, что антивирусные базы актуальны, в противном случае – обновить их.

оставляя рабочее место без наблюдения блокировать доступ к компьютеру средствами операционной системы (заблокировать компьютер).

4.1.2. При работе с электронными письмами запрещается:

открывать электронные письма от неизвестных адресатов;

открывать письма с неизвестных адресов или преднамеренно искаженных адресов;

открывать письма с призывами к действию (например, «открой», «прочитай», «внимание» и т.д.);

переходить по ссылкам, содержащимся в электронных письмах (особенно если они слишком длинные или используют сервисы сокращения ссылок bit.ly, tinyurl и др.);

открывать вложения к электронным письмам, содержащие макросы, архивы, исполняемые файлы (файлы с расширением exe/zip/rar/msi/bat/sh/7z) от недоверенных источников.

4.1.3. При работе с сайтами в сети Интернет запрещается:

посещать сайты с личными целями, не связанными с осуществлением трудовой деятельности;

посещать сайты, потенциально угрожающие информационной безопасности (фишинговые сайты, вредоносные сайты и т.д.).

4.2. К грубым нарушениям правил работы в Интернет относятся:

установка имен рабочей станции или домена, не удовлетворяющих принятым правилам наименования рабочих станций, доменов и рабочих групп;

обход учетных систем получаемого трафика, их повреждение или дезинформация;

работа в сети Интернет без использования средств антивирусной защиты, а в случаях, предусмотренных локальными нормативными актами университета в области защиты персональных данных, без средств криптографической защиты информации;

преднамеренная рассылка вирусов через сеть Интернет;

предоставление служебной информации для общего доступа;

несанкционированное предоставление персональных данных (логинов, паролей, IP адресов и т.д.) для общего доступа;

предоставление любой информации в общий доступ на рабочей станции (информацию для общего доступа разрешается размещать на официальном сайте университета по установленным правилам);

установка и/или удаление сетевого программного обеспечения без согласования с системными администраторами университета;

использование социальных сетей в личных целях, не связанных с осуществлением трудовой деятельности;

доступ в сеть Интернет в неустановленное время;

распространение через сеть Интернет информации, запрещенной действующим законодательством или не соответствующей морально-этическим нормам ее получателей, а также рассылка обманных, беспокоящих или угрожающих сообщений и рассылка незапрашиваемых сообщений (спама) за исключением служебных сообщений.

4.3. В случае возникновения угроз информационной безопасности, отклонениях в работе КИС, возникших угрозах информационной безопасности, неправомерных действиях третьих лиц (угрозы, попытки подкупа или получения доступа к конфиденциальной информации) необходимо незамедлительно сообщить в отдел компьютерных технологий.

5. Публикация служебной и конфиденциальной информации

5.1. Запрещается публиковать для всеобщего доступа детальную служебную и конфиденциальную информацию, а также информацию, касающуюся устройства и архитектуры локальной вычислительной сети, в т.ч. схемы локальной вычислительной сети и ее сегментов, точек подключения, информацию о назначенных рабочим станциям IP адресах и именах, используемых на серверах, средствах удаленного доступа и т.д., а также информацию о каналах связи между учебными корпусами университета.

5.2. Запрещается несанкционированная публикация в открытом доступе персональных данных.

6. Ответственность

6.1. Контроль за соблюдением настоящих правил возлагается на отдел компьютерных технологий. В случае выявления нарушений и злоупотреблений могут быть применены нижеуказанные меры на установленный период или до устранения причин, повлекших за собой принятие настоящих мер:

персонально к нарушителю:
отключение доступа в Интернет;
лишение возможности работы за компьютером;
уменьшение ежемесячной нормы потребления трафика;
ограничение доступа к информационным ресурсам Интернет;
ограничение на использование электронной почты;
принятие административных мер воздействии;

к рабочей станции или серверу:
отключение доступа в сеть Интернет;
отключение возможности работы в локальной сети;
физическое отключение от КИС;
удаление информации из общего доступа.

6.2. При работе в сети любые действия пользователя не должны вступать в противоречие с Законодательством РФ, в частности, с положением статей Уголовного кодекса РФ, касающихся преступлений в сфере компьютерной информации, запрещения распространения порнографии, национальной дискриминации и призывов к насилию.

6.3. В случае разглашения сведений, имеющих ограниченное распространение, пользователь несет ответственность в соответствии с действующим Законодательством РФ и локальными нормативными актами университета.

Согласовано:

Проректор по инновационной работе
_____ И.А. Лагерев
«04» 07 2022 г.

Начальник отдела компьютерных технологий
_____ С.В. Антоненко
«04» 07 2022 г.

Начальник юридического отдела
Сенино Д.С. Мельников
«04» 07 2022 г.

Лист ознакомления с инструкцией
по правилам работы сотрудников университета в сети Интернет
от «___»_____ 2022 г.,
об ответственности за нарушение требований в области информационной безопасности и разглашение конфиденциальной информации

№ п/п	Фамилия, И.О.	Должность	Дата	Подпись