КОМИТЕТ ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ЛЕНИНГРАДСКОЙ ОБЛАСТИ
Государственное бюджетное профессиональное образовательное учреждение Ленинградской области «Беседский сельскохозяйственный техникум»
(ГБПОУ ЛО «Беседский сельскохозяйственный техникум»)

УТВЕРЖДАЮ:
Директор
_____ Н.Н. Казанцев
распоряжение от «07» июня 2023 г. № 69

ПОЛОЖЕНИЕ

об информационной безопасности
в ГБПОУ ЛО «Беседский сельскохозяйственный техникум»

1. Общие положения

1.1. Настоящее Положение об информационной безопасности в ГБПОУ ЛО «Беседский сельскохозяйственный техникум» (далее Положение) является локальным нормативным актом государственного бюджетного профессионального образовательного учреждения Ленинградской области «Беседский сельскохозяйственный техникум» (далее – техникум), разработанным в соответствии с целями, задачами и принципами обеспечения информационной безопасности образовательного учреждения.

1.2. Целью настоящего Положения, является обеспечение безопасности объектов защиты техникума от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональным данным.

1.3. Информационная безопасность достигается путем исключения несанкционированного или случайного доступа к служебной информации и персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.4. Организационное и техническое обеспечение рабочего процесса сотрудников техникума возлагается на сетевого администратора.

2. Порядок установки оборудования и программного обеспечения (ПО)

2.1. Установка и обслуживание оборудования возможна только сетевым администратором либо лицом, ответственным за проведение работ.

2.2. Установка и обслуживание оборудования другими сотрудниками техникума запрещена.

2.3. Установка ПО возможна только сетевым администратором либо лицом, ответственным за проведение работ.

2.4. Установка ПО другими сотрудниками техникума запрещена.

3. Порядок мероприятий по обновлению ПО

3.1. Комплекты обновлений должны быть получены только от разработчика программного обеспечения. Запрещается получать обновления программного обеспечения из недостоверных источников.

3.2. Обновление программного обеспечения проводится сетевым администратором, либо лицом, ответственным за проведение работ по обновлению программного обеспечения, с участием специалистов техникума.

3.3. До начала проведения работ по обновлению сетевой администратор проводит работы по резервному копированию ПО и баз данных ИС.

3.4. Сетевой администратор должен придерживаться рекомендациям по обновлению ПО, описанных в соответствующей технической и эксплуатационной документацией к программному обеспечению, инструкции по установки обновления (при наличии) или рекомендациям по обновлению программного обеспечения от разработчика.

3.5. Мониторингом выхода актуальных обновлений на ПО и анализом возможности их установки осуществляется сетевым администратором, либо лицом, ответственным за проведение работ по обновлению программного обеспечения.

3.6. По завершению мероприятий по обновлению ПО необходимо проверить работоспособность основного функционала программного обеспечения. При обнаружении ошибок и нарушения функционирования ПО сетевым администратором производится восстановление ПО и базы данных из резервной копии.

4. Учётные записи

4.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику техникума, допущенному к работе с конкретной информационной системой, должно быть сопоставлено персональное уникальное имя - учётная запись пользователя и пароль, под которым он будет регистрироваться и работать в системе.

4.2. К специальным учетным записям относятся:

- реквизиты доступа к активному сетевому оборудованию;
- учетные записи для доступа к базам данным, различным информационным системам используемых в управленческом и учебном процессах.

4.3. Создание специальных учетных записей производится сетевым администратором при возникновении необходимости.

5. Требования к паролям

5.1. Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи. Установку первичного пароля производит сетевой администратор при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на сетевом администраторе.

5.2. Основной пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы) известная только сотруднику техникума, используемая для подтверждения подлинности владельца учетной записи.

5.3. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

5.4. При выборе пароля необходимо руководствоваться следующими правилами:

- длина пароля должна составлять не менее 8 символов;
- при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов;
- запрещается использовать в качестве пароля название учетной записи, фамилию или имя пользователя, а также легко угадываемые сочетания символов.

5.5. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, записывать его, а также пересылать открытым текстом в электронных сообщениях.

5.6. Пользователь обязан не реже одного раза в три месяца производить смену основного пароля, соблюдая требования настоящего Положения.

5.7. Восстановление забытого основного пароля пользователя осуществляется сетевым администратором путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной заявки пользователя.

5.8. Разблокирование учетной записи пользователя осуществляется сетевым администратором на основании заявки владельца учетной записи.

5.9. Административный пароль - комбинация символов, используемая при настройке служебных учетных записей, учетных записей служб и сервисов, а также специальных учетных записей. Административный пароль устанавливает сетевой администратор. Сетевой администратор несет персональную ответственность за сохранение в тайне административного пароля. Сетевой администратор обязан не реже одного раза в месяц производить смену административного пароля.

6. Доступ к ресурсам сети Интернет

6.1. Для исполнения задач, связанных с производственной деятельностью сотрудникам техникума, предоставляется доступ к ресурсам Интернет. Доступ к ресурсам сети Интернет в других целях запрещен.

6.2. Доступ к ресурсам Интернет может быть блокирован сетевым администратором без предварительного уведомления при возникновении нештатных ситуаций, либо в иных случаях, предусмотренных организационными документами.

6.3. Сетевой администратор обязан не реже одного раза в месяц представлять отчет об использовании Интернет-ресурсов сотрудниками директору техникума.

7. Электронная почта

7.1. Для исполнения задач, связанных с производственной деятельностью сотрудникам техникума может быть предоставлен доступ к системе электронной почты. Использование системы электронной почты техникума в других целях запрещено.

7.2. Доступ к системе электронной почты предоставляется сотруднику техникума на основании заявки на имя директора техникума.

7.3. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию директора техникума либо вышестоящего руководства.

7.4. В случае обнаружения значительных отклонений в параметрах работы средств обеспечения работы системы электронной почты, сетевой администратор обязан немедленно сообщить об этом директору техникума для принятия решений.

7.5. Доступ к серверу электронной почты может быть блокирован сетевым администратором без предварительного уведомления при возникновении нештатных ситуациях, либо в иных случаях, предусмотренных организационными документами.

8. Антивирусная защита

8.1. К использованию в техникуме допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

8.2. Установка средств антивирусного контроля на компьютерах (серверах ЛВС) техникума осуществляется.

8.3. Настройка параметров средств антивирусного контроля осуществляется сетевым администратором в соответствии с руководствами по применению конкретных антивирусных средств. Изменение настроек другими сотрудниками запрещено.

8.4. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов персональных компьютеров. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях.

8.5. Антивирусная проверка должна проводиться:

- на компьютерах сотрудников – не реже одного раза в неделю;
- на серверах ЛВС (при наличии такового) — не реже двух раз в неделю.

8.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник техникума должен самостоятельно провести внеочередной антивирусный контроль своей рабочей станции.

9. Хранение данных

9.1. Для хранения информации, используемой в профессиональной деятельности, на компьютере сотрудника должны быть созданы тематические папки. Возможно выделение сетевых папок на сервере техникума (при наличии такового). Хранение личной информации в служебных папках запрещено.

9.2. Сотрудникам техникума для обеспечения целостности данных необходимо проводить резервное копирование не реже одного раза в сутки. Резервное копирование личной информации не предусмотрено.

10. Ответственность пользователей

10.1. Ответственность за обеспечение целостности данных, хранимых на серверах техникума (при наличии таковых) в соответствии с требованиями настоящего положения возлагается на сетевого администратора.

10.2. Ответственность за обеспечение целостности данных, хранимых на локальных компьютерах сотрудников техникума возлагается на самих сотрудников.

Приложение 1

ПАСПОРТ
программного обеспечения, используемого
в ГБПОУ ЛО «Бокситогорский сельскохозяйственный техникум»

№ п/п	Классификация ПО	Наименование ПО	Схема лицензирования
1.	Операционные системы	Microsoft Windows 7	OEM. BOX
		Microsoft Windows 10	OEM. BOX
2.	Офисные приложения	Microsoft Office 2007	OLP
		Open Office	Свободное ПО
		Adobe Acrobat Reader	Бесплатное ПО
3.	Антивирусное ПО	Kaspersky Endpoint Security	Лицензия
		Kaspersky Antivirus	Лицензия
		360 Total Security	Бесплатное ПО
4.	Браузеры	Яндекс	Свободное ПО
		Google Chrome	Свободное ПО
5.	Специализированное ПО	1С Предприятие	Лицензия
		Система Госфинансы	Лицензия
		Система Кадры	Лицензия
		Компас 3D	Версия для учебных заведений
		AutoCad	Версия для учебных заведений

Приложение 2

Правила
работы персонала и обучающихся техникума в компьютерных сетях

1. Данные правила регулируют права и обязанности обучающихся, связанные с работой в компьютерной сети техникума и сети Интернет (далее Сетей), а также основные правила работы и полномочия преподавателей и сотрудников техникума. Правила призваны обеспечить и организовать использование образовательного потенциала Сетей в сочетании с системой мер по обеспечению охраны и безопасности обучающихся.
2. Основными принципами для работы в Сетях являются:
   - равный доступ для всех обучающихся;
   - использование Сетей обучающимися только для образовательных целей;
   - защита обучающихся от вредной или незаконной информации, содержащей: порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр и т.п.
3. Правила работы в Сетях должны быть расположены в каждом компьютерном классе.
4. Полномочия сотрудников и педагогических работников

4.1. Заместители директора техникума, заведующие отделениями:
   - обеспечивают свободный и равный доступ обучающихся к Сетям в соответствии с профессиональной образовательной программой и возможностями техникума;
   - создают возможности для обогащения и расширения образовательного процесса через Сети;
   - обеспечивают контроль за соблюдением правил работы, обучающихся в сетях;
   - организуют в начале каждого учебного года ознакомление обучающихся с правилами безопасной работы в Сети. Информируют обучающихся, что трафик контролируется;
   - организуют поддержку и обновление официального сайта техникума;
   - незамедлительно сообщают директору техникума о выявлении нарушений в сфере информационной безопасности и принимают меры по устранению нарушений;
   - могут делегировать свои обязанности сетевому администратору.

4.2. Педагогические работники обязаны:
   - объяснять обучающимся правила безопасного и ответственного поведения при работе в Сетях;
   - использовать возможности сети Интернет в целях обогащения и расширения образовательной деятельности, для чего обучающимся назначать конкретные задания и приводить перечень соответствующих интернет-адресов;
   - своевременно подавать заявки на предоставление доступа для группы обучающихся в пределах учебных занятий, предусмотренных календарно-тематическими планами, а также для открытия доступа вне учебных планов с указанием перечня необходимых ресурсов с обоснованием;
   - осуществлять непрерывный контроль работы обучающихся в Сетях в учебное время;
   - принимать незамедлительные меры для прекращения доступа обучающихся к ресурсам запрещенного содержания в Сетях;
   - немедленно сообщать о нарушении правил или о создании незаконного контента в сети техникума;
   - не покидать учебный кабинет (лабораторию) во время пары, и не допускать обучающихся во время перемены к работе в Сетях.

4.3. Педагогические работники несут ответственность за целостность оборудования техникума, закрепленного за учебным кабинетом (лабораторией), в котором проводят занятия.

4.4. Сетевой администратор обязан:

- обеспечивать общую безопасность и эффективность работы в Сетях;
- предлагать и осуществлять меры по ограничению доступа обучающихся к вредным или незаконного содержания ресурсам в Сетях в соответствии с законодательством;
- периодически просматривать содержимое Сети техникума с целью предотвращения любых возможных угроз и рисков безопасности для обучающихся;
- осуществлять мониторинг трафика;
- немедленно сообщать директору техникума о нарушении Правил или о создании незаконного контента в сети техникума.

5. Права и обязанности обучающихся

5.1. Обучающиеся имеют право:

- на равный доступ к Сетям с учетом политики информатизации техникума;
- на получение доступа к сети Интернет (только под наблюдением преподавателя);
- на грамотное и ответственное обучение работе в Сетях;
- быть информированным о правилах работы в Сетях.

5.2. Обучающиеся обязаны соблюдать следующие правила:

- использовать Сети только для образовательных целей;
- запрещается выход на сайты, не включенные в перечень преподавателем для данного занятия;
- немедленно сообщить преподавателю при обнаружении материалов, содержащих порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр, и т.п.;
- не должны отправлять или отвечать на сообщения, оскорбительные, угрожающие или непристойные;
- запрещается проводить любую деятельность, которая угрожает целостности компьютерной сети техникума или атаки на другие системы;
- запрещается использование чужих имен пользователя, пароля и электронной почты;
- запрещено использование нелицензионного программного обеспечения, защищенных авторским правом материалов без разрешения, и любой другой деятельности, которая нарушает авторские права.

6. Ответственность пользователей

6.1. Обучающиеся за нарушение положений настоящих Правил привлекаются к дисциплинарной ответственности в соответствии с правилами внутреннего распорядка техникума.

6.2. Преподаватели и сотрудники за нарушение положений настоящих Правил несут ответственность в соответствии с Трудовым кодексом и привлекаются к дисциплинарной ответственности.

6.3. За нарушения, которые являются преступлениями, административными нарушениями или причиняют ущерб собственности, виновные несут ответственность в соответствии с законодательством РФ.

Приложение 3

Правила
работы с ресурсами сети Интернет

1. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. техникума имеет право ограничивать доступ к ресурсам сети Интернет. содержание которых не имеет отношения к исполнению служебных обязанностей. а также к ресурсам. содержание и направленность которых запрещены международным и Российским законодательством включая материалы. носящие вредоносную. угрожающую. клеветническую. непристойную информацию. а также информацию. оскорбляющую честь и достоинство других лиц. материалы. способствующие разжиганию национальной розни. подстрекающие к насилию. призывающие к совершению противоправной деятельности. в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия. и т.д.
2. При работе с ресурсами сети Интернет недопустимо:
   - разглашение коммерческой и служебной информации техникума. ставшей известной сотруднику техникума по служебной необходимости либо иным путем;
   - распространение защищаемых авторскими правами материалов. затрагивающих какой-либо патент. торговую марку. коммерческую тайну. копирайт или прочие права собственности и или авторские и смежные с ним права третьей стороны;
   - публикация. загрузка и распространение материалов. содержащих вирусы или другие компьютерные коды. файлы или программы. предназначенные для нарушения. уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ. для осуществления несанкционированного доступа. а также серийные номера к коммерческим программным продуктам и программы для их генерации. логины. пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете. а также размещения ссылок на вышеуказанную информацию.
3. При работе с ресурсами Интернет запрещается:
   - загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
   - использовать программные и аппаратные средства. позволяющие получить доступ к ресурсу. запрещенному к использованию в образовательной организации.
4. Возможность получить доступ к ресурсу не является гарантией того. что запрошенный ресурс является разрешенным к использованию в образовательном процессе или профессиональной деятельности сотрудника техникума.
5. Вся информация о ресурсах. посещаемых сотрудниками техникума. протоколируется и. при необходимости. может быть предоставлена руководителям подразделений. а также администрации техникума для детального изучения.

Приложение 4

Правила
работы с электронной почтой

1. Электронная почта является собственностью техникума и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.
2. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.
3. При работе с корпоративной системой электронной почты сотрудникам техникума запрещается:
   - использовать адрес корпоративной почты для оформления подписок и массовых рассылок;
   - публиковать свой адрес, либо адреса других сотрудников техникума на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
   - отправлять сообщения с вложенными файлами, общий объем которых превышает 5 Мегабайт;
   - открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
   - осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;
   - осуществлять массовую рассылку почтовых сообщений рекламного характера, рассылку материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;
   - распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей сторон;
   - распространять информацию содержание и направленность которой запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;
   - распространять информацию ограниченного доступа, представляющую коммерческую тайну;
   - предоставлять кому бы то ни было пароль для доступа к своему почтовому адресу.