УТВЕРЖДАЮ
Начальник главного управления по образованию облисполкома
Н.Н.Башко

ПОЛОЖЕНИЕ
о порядке защиты информации в учреждениях образования Минской области

1. В настоящем Положении, разработанном в соответствии с пунктом 3 Плана по реализации на территории Минской области Комплексного плана мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2021-2022 годы, утвержденного заместителем председателя Минского областного исполнительного комитета 28 апреля 2021 года, устанавливается комплекс организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации, обрабатываемой в учреждении образования.

2. Для целей настоящего Положения термины и их определения применяются в значениях, установленных Законом Республики Беларусь от 10 ноября 2008 года № 455-З «Об информации, информатизации и защите информации» (Национальный реестр правовых актов Республики Беларусь, 2008 г., № 279, 2/1552) и Законом Республики Беларусь от 7 мая 2021 года № 99-З «О защите персональных данных» (Национальный реестр правовых актов Республики Беларусь, 2021 г., № 2/2819).

3. Действие настоящего Положения направлено на защиту общедоступной информации, информации о частной жизни и персональных данных обучающихся, их законных представителей, педагогических работников и иных работников учреждения образования, а также информации, составляющей служебную и коммерческую тайну учреждения образования.

4. За общее состояние, организацию и контроль работ по реализации комплекса мер по защите информации отвечает один из заместителей руководителя учреждения образования или другое должностное лицо, уполномоченное приказом руководителя учреждения образования.

5. Для недопущения неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или)

предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий должны выполняться мероприятия по защите объектов информационной среды (далее – ОИС) учреждения образования.

6. Под ОИС понимаются средства вычислительной техники (далее – СВТ), сетевое оборудование, системное и прикладное программное обеспечение, информационные ресурсы и системы учреждения образования.

7. Субъектами информационной среды учреждения образования являются педагогические работники, иные работники учреждения образования, обучающиеся и их законные представители (далее – пользователи).

8. Защита ОИС должна содержать:

обеспечение защиты СВТ от вредоносного программного обеспечения;

отключение функции автозагрузки внешних машинных носителей информации при их подключении к СВТ;

использование ОИС с правами пользовательских учетных записей;

обеспечение управления (централизованного) (создание, активация, блокировка, уничтожение) учетными записями пользователей для доступа к ОИС;

ограничение возможности использования общих учетных записей пользователей для доступа к ОИС;

разграничение доступа пользователей к ОИС;

ограничение возможности установки программного обеспечения под учетными записями пользователей;

обеспечение идентификации и аутентификации пользователей информационных ресурсов учреждения образования для организации заочного (дистанционного) обучения;

своевременную блокировку (уничтожение) неиспользуемых (временно неиспользуемых) учетных записей пользователей;

обеспечение доступа пользователей к ОИС на основе ролей;

блокирование доступа к ОИС после истечения установленного времени бездействия (неактивности) пользователя или по его запросу;

обеспечение управления физическим доступом в помещения, а также к шкафам со СВТ, сетевым и другим оборудованием;

предоставление уникальных учетных записей привилегированным пользователям для авторизованного доступа к сетевому оборудованию и установки программного обеспечения;

предоставление пользователям авторизованного доступа при подключении к ОИС из-за ее пределов;

использование услуг хостинга уполномоченных поставщиков интернет-услуг;

размещение существующих, создаваемых (приобретаемых, модернизируемых) информационных ресурсов и систем учреждения образования в республиканском центре обработки данных;

регламентирование порядка работы с интернет-сайтом учреждения образования и корпоративной электронной почтой;

обеспечение в реальном масштабе времени автоматической антивирусной проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживания обнаруженных вредоносных программ;

обеспечение спам-фильтрации почтовых сообщений;

ограничение входящего и исходящего трафика (фильтрация) определенных приложений и сервисов (мессенджеры, социальные сети, онлайн-маркеты, анонимайзеры и др.);

обеспечение доступа пользователей в сеть Интернет с применением технологии проксирования сетевого трафика;

использование ОИС локальной системы доменных имен (DNS-сервер), в том числе для доступа в сеть Интернет, либо системы доменных имен, расположенной на территории Республики Беларусь;

определение состава и содержания информации, подлежащей резервированию (в том числе конфигурационных файлов сетевого оборудования, лог-файлов служб и сервисов);

обеспечение резервирования информации;

осуществление синхронизации системного времени от единого источника;

обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и физической сети, а также виртуальных машин;

обучение работников учреждения образования правилам использования почтовых сервисов, определения фишинговых сообщений и т.п.;

проведение не менее одного раза в год с работниками учреждения образования практических занятий по правилам безопасной работы с ОИС.

9. Управление полномочиями доступа пользователей либо групп пользователей к ОИС осуществляется привилегированными пользователями (администраторами) из числа работников учреждения образования, имеющих соответствующую профессиональную подготовку и (или) опыт работы.

10. Учреждение образования выступает в роли оператора персональных данных педагогических работников, иных работников учреждения образования, обучающихся и их законных представителей и

осуществляет обработку персональных данных в соответствии с действующим законодательством.

11. Внутренний контроль за обработкой персональных данных выполняет ответственный за общее состояние, организацию и контроль работ по реализации комплекса мер по защите информации.

12. Обеспечение защиты персональных данных от несанкционированного или случайного доступа к ним, изменения, блокирования, копирования, распространения, предоставления, удаления персональных данных, а также от иных неправомерных действий в отношении персональных данных должно включать:

издание в учреждении образования регламента обработки персональных данных;

ознакомление работников учреждения образования, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе с требованиями по защите персональных данных, регламентом обработки персональных данных, а также обучение указанных работников и лица, осуществляющего внутренней контроль за обработкой персональных данных, в порядке, установленном законодательством;

установление порядка доступа к персональным данным;

при передаче технических средств для проведения ремонта из этих технических средств изымаются все носители информации, содержащие персональные данные, либо должно быть произведено гарантированное уничтожение информации.

13. В целях недопущения уничтожения, модификации (изменения), блокирования правомерного доступа к общедоступной информации на интернет-сайте учреждения образования из числа работников учреждения образования назначаются лица, уполномоченные осуществлять администрирование и размещение информации на интернет-сайте, и устанавливается их персональная ответственность за использование интернет-сайта для целей, не предназначенных для выполнения служебных задач.

14. Для официальной переписки с вышестоящими государственными органами и (или) организациями используется система межведомственного оборота и корпоративная электронная почта. В учреждении образования определяются технические средства, на которых выполняется работа по официальной переписке, из числа работников учреждения образования назначаются лица, уполномоченные осуществлять эту работу.

15. Требования настоящего Положения являются обязательными для исполнения всеми работниками учреждения образования.

16. Работники учреждения образования:

не имеют права разглашать, передавать другим лицам свои пароли от учетных записей для доступа к техническим средствам, информационным ресурсам и системам;

несут персональную ответственность за действия, совершенные под их учетными записями, за исключением случаев несанкционированного использования паролей.

17. В должностные инструкции работников учреждения образования вносятся дополнения в соответствии с пунктами 4, 9, 11, 13-16 настоящего Положения.

18. Пункты 10-12 настоящего Положения вступают в силу с 15 ноября 2021 года.