Государственное учреждение образования «Академия образования»

УТВЕРЖДЕНО
Приказ ректора
21.06.2024 № 226

ПОЛИТИКА
информационной безопасности в Государственном учреждении образования «Академия образования»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Система информационной безопасности в Государственном учреждении образования «Академия образования» (далее – Академия образования) как организованная совокупность специальных средств, методов и мероприятий, предназначена для:

прогнозирования, своевременного выявления и устранения угроз профессионально значимым ресурсам и информационным системам Академии образования на основе правовых, организационных и инженерно-технических мер, а также средств обеспечения защиты;

минимизации ущерба и оперативного восстановления программных и аппаратных средств, информации, пострадавших в результате кризисных ситуаций, выявление причин возникновения таких ситуаций и принятие соответствующих мер по их предотвращению;

идентификации и регламентации доступа к сетевым ресурсам, в том числе к ресурсам глобальной компьютерной сети Интернет;

предотвращения критических последствий несанкционированного распространения, уничтожения, искажения, копирования данных;

сбора, хранения и анализа данных об использовании сетевых ресурсов и сервисов, предоставления соответствующей статистической информации.

1.2. Настоящий документ разработан в соответствии со следующими нормативными правовыми и иными актами:

Законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

Законом Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»;

приказом оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»;

приказом оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 «О технической и криптографической защите персональных данных»;

иными нормативными правовыми актами Республики Беларусь в области электросвязи, информатизации, безопасности и защиты информации, международные стандарты в области информационной безопасности продуктов и систем информационных технологий.

1.3. Политика информационной безопасности в Академии образования (далее – Политика) представляет собой совокупность правил, процедур и требований в области защиты информации, действующих в Академии образования.

1.4. Политика определяет основы сетевой политики и информационной компьютерной безопасности, порядок доступа и правила работы пользователей персональных компьютеров с ресурсами локальной сети и глобальной компьютерной сети Интернет в Академии образования.

1.5. Контроль за исполнением мероприятий по информационной безопасности в Академии образования осуществляет проректор по учебной работе.

1.6. Сотрудники Академии образования несут личную ответственность за соблюдение правил информационной безопасности, определяемых настоящим положением. Ответственность за обеспечение выполнения настоящей Политики в структурных подразделениях возлагается на руководителей этих подразделений.

1.7. В Политику могут вноситься изменения и дополнения в связи с изменениями законодательства Республики Беларусь, а также технических нормативных актов, обязательных к применению.

1.8. Политика информационной безопасности Академии образования предполагает реализацию принципов конфиденциальности информации (недоступности ее третьим лицам); целостности информации (недопущение искажений или подмены); доступности информации (реализация возможности для пользователей иметь доступ к нужным данным).

1.9. Целью Политики является защита информации от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи; регламентирование основных принципов и единых подходов для обеспечения выполнения требований информационной безопасности в деятельности Академии образования.

1.10. Достижение указанной цели предполагает решение следующих задач:

реализация требований законодательства Республики Беларусь в части информационной безопасности информационных систем и мер контроля их защищенности;

определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований Политики, в том числе с использованием программных, программно-аппаратных средств технической и криптографической защиты информации, а также посредством принятия соответствующих внутренних нормативных и организационно-методических документов информационной безопасности Академии образования;

своевременное выявление и оценка причин, условий и характера угроз информационной безопасности и дальнейшее прогнозирование развития событий на основе мониторинга инцидентов информационной безопасности;

планирование, реализация и контроль эффективности использования защитных мер и средств защиты информации, создание механизма оперативного реагирования на угрозы информационной безопасности;

реализация программ по осведомленности и обучению сотрудников Академии образования о возможных факторах рисков информационной безопасности и мерах противодействия угрозам безопасности.

ГЛАВА 2
ОРГАНИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. В локальной сети Академии образования выделены три изолированных сегмента:

2.1.1. сегмент локальной сети компьютерных классов Академии образования (корпус Некрасова, 20) для обмена данными при реализации образовательного процесса, подключенный к открытому каналу передачи данных;

2.1.2. сегмент локальной сети Академии образования (корпус Некрасова, 20) в пределах рабочих мест сотрудников для обмена необходимыми данными при выполнении своих должностных обязанностей, подключенный к открытому каналу передачи данных;

2.1.3. сегмент локальной сети Академии образования (корпус Короля, 16) в пределах рабочих мест сотрудников для обмена необходимыми данными при выполнении своих должностных обязанностей, подключенный к открытому каналу передачи данных.

Информационные потоки сегментов локальной сети, имеющие подключение к открытым каналам передачи данных, регулируются серверным программным обеспечением.

2.2. Уполномоченной комиссией (приказ ректора от 19.06.2024 № 222) составлены акты отнесения информационных систем Академии образования к классу типовых информационных систем:

2.2.1. Класс 4-ин (информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые не имеют подключений к открытым каналам передачи данных) – Система сопровождения деятельности Академии образования:

локальная система управления учебным процессом в Академии образования (планирование, регистрация и анкетирование слушателей, учет учебной нагрузки и т.п.),

локальная система резервного копирования;

программное обеспечение учета кадров «DELTA+персонал».

2.2.2. Класс 5-гос (государственные информационные системы, в которых обрабатывается общедоступная информация и которые подключены к открытым каналам передачи данных) – Цифровая образовательная среда Академии образования:

Официальный сайт государственного учреждения образования «Академия образования» (регистрационный № 1180300253 от 15.09.2003 с изменениями 2024 года в Государственном регистре информационных ресурсов),

Система дистанционного обучения государственного учреждения образования «Академия последипломного образования» (регистрационный № 1141303644 от 06.11.2013 с изменениями 2024 года в Государственном регистре информационных ресурсов),

Диагностика профессиональной компетентности воспитателя дошкольного образования (регистрационный № 1141918192 от 29.04.2019 с изменениями 2024 года в Государственном регистре информационных ресурсов),

Национальный образовательный портал (регистрационный № 1141609129 от 06.07.2016 с изменениями 2024 года в Государственном регистре информационных ресурсов).

2.3. Для обмена сообщениями электронной почты с высоким уровнем безопасности в Академии образования подключена услуга корпоративной почты, позволяющая обеспечивать надежное хранение данных, безопасную передачу сообщений по SSL-протоколу, защиту почтового трафика.

Для выполнения служебных обязанностей сотрудники Академии образования обязаны пользоваться официальными электронными ящиками (@akademy.by и(или) @adu.by).

Корпоративная электронная почта для сотрудников Академии образования предназначена для ведения служебной и деловой переписки. Использование корпоративной почты в личных целях запрещено.

2.4. Организация и обеспечение эффективности функционирования системы информационной безопасности в Академии образования возлагается на центр планирования и информационного сопровождения образовательного процесса и центр информационных образовательных технологий.

2.5. Начальники центра планирования и информационного сопровождения образовательного процесса и центра информационных образовательных технологий по согласованию с ректором Академии образования определяют основные положения сетевой политики и технологии ее реализации. Функции оперативного управления техническими ресурсами системы защиты информации возлагаются на специально назначенных сотрудников центра планирования и информационного сопровождения образовательного процесса и центра информационных образовательных технологий (уполномоченных сотрудников).

2.6. Уполномоченный сотрудник имеет право по согласованию с ректором Академии образования проводить специальные технические мероприятия для выявления попыток повреждения оборудования, взлома программного обеспечения и несанкционированного доступа к ресурсам локальной сети или глобальной компьютерной сети Интернет.

2.7. Уполномоченный сотрудник обязан:

знать и правильно использовать серверное программное обеспечение, аппаратно-программные средства защиты информации и обеспечивать сохранность информационных ресурсов с помощью этих средств;

обеспечивать бесперебойную работу основных сетевых сервисов, производить необходимые настройки и корректировки серверного программного обеспечения;

осуществлять регулярный мониторинг параметров состояния локальной сети, обеспечивать ее бесперебойное функционирование;

выполнять установку и регулярное обновление антивирусных программ, иных программных средств, необходимых для безопасного доступа к глобальной компьютерной сети Интернет;

тестировать рабочие станции локальной сети на предмет наличия вредоносных программ;

осуществлять сбор и анализ серверных протоколированных данных о выполненных подключениях и использовании ресурсов глобальной компьютерной сети Интернет, обеспечивать хранение соответствующей статистической информации в течение календарного года;

консультировать и осуществлять техническую поддержку пользователей по вопросам использования сетевых ресурсов и сервисов;

сообщать руководству о выявленных фактах применения пользователями программных продуктов, приводящих к сбоям в работе

компьютерного и/или сетевого оборудования, предназначенных для несанкционированного доступа, модификации, разрушения информационных ресурсов.

2.8. Для каждого персонального компьютера в подразделениях Академии образования определяется ответственное лицо из штатного состава соответствующих подразделений. На всех персональных компьютерах Академии образования настроен тип учетной записи с парольной защитой, включено ведение системного журнала событий.

ГЛАВА 3
ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Внешние и VPN каналы передачи данных предоставляются Академии образования на договорной основе через провайдера, имеющего государственные лицензии на осуществление соответствующих видов деятельности с учетом всех требований законодательства, в том числе требований информационной безопасности. Для сетевого оборудования сразу после установки осуществляется смена реквизитов доступа к функциям управления и настройкам, установленным по умолчанию.

3.2. Персональные компьютеры закрепляются в помещениях Академии образования за строго определенными рабочими местами и идентифицируются в локальной сети на основании фиксированных IP-адресов (корпус Некрасова, 20) и на основании учетных записей (корпус Короля, 16).

3.3. Идентификация пользователей сети обеспечена средствами операционных систем, установленных на устройствах пользователей. Аутентификация пользователей обеспечивается модулями авторизации информационных систем, используемых в Академии образования.

3.4. Применение специализированного программного обеспечения доступа пользователей локальной сети Академии образования в глобальной компьютерной сети Интернет разрешается только через внутренний контролируемый прокси-сервер (корпус Некрасова, 20) и сервер домена локальной сети (корпус Короля, 16).

3.5. Определен минимальный перечень разрешенного программного обеспечения для сегментов локальной сети Академии образования в составе:

3.5.1. для сегмента сети из п.2.1.1 настоящей Политики:

Microsoft Windows;

Microsoft Office;

системы антивирусной защиты;

3.5.2. для сегмента сети из п.2.1.2 настоящей Политики:

Microsoft Windows;

Microsoft Office;

системы антивирусной защиты;

Информационно-правовая система «ILEX» – управление бухгалтерского учета и финансов, юридический сектор, планово-экономическое управление;

Автоматизирования система «Электронное дело» – отдел делопроизводства и документооборота, ректорат;

Система межведомственного документооборота (СМДО) – отдел делопроизводства и документооборота;

Программное обеспечение учета кадров «DELTA+персонал» – отдел кадров;

Автоматизированная система управления бухучетом «1С» – управление бухгалтерского учета и финансов.

3.5.3. для сегмента сети из п.2.1.3 настоящей Политики:

Microsoft Windows;

Microsoft Office;

системы антивирусной защиты.

3.6. Для обмена информацией между пользователями в пределах сегментов локальной сети используется специально настроенные области памяти на файловых серверах Академии образования (сетевые диски). Сетевые диски не предназначены для размещения конфиденциальных данных и длительного хранения информации.

3.7. Доступ пользователей к ресурсам глобальной компьютерной сети Интернет регламентируется прокси-сервером (корпус Некрасова, 20) и сервером домена локальной сети (корпус Короля, 16). Настройки прокси-сервера задают необходимые разрешения по скорости, объему трафика и времени доступа, устанавливают запреты на посещение определенных ресурсов.

3.8. Все сеансы выхода в глобальную компьютерную сеть Интернет фиксируются в логах прокси-сервера. Для анализа и обработки логов на сервере устанавливается специализированное программное обеспечение. Запрет на доступ к определенным ресурсам сети Интернет осуществляется провайдером, предоставляющим услугу подключения к сети Интернет.

3.9. На серверах Академии образования выполняется автоматизированный сбор и хранение информации о событиях информационной безопасности в виде протокола серверных логов, регистрирующих обращения к серверу и возникающие при этом ошибки, логи баз данных, фиксирующие запросы к базам данных, логи авторизации и аутенфикации.

3.10. Не реже одного раза в месяц проводится анализ и оперативная корректировка списков разрешений на доступ к Интернет-ресурсам,

проводится анализ состояния локальной сети, выполняются профилактические работы.

3.11. По мере необходимости обновляются операционные системы, корректируются методики использования серверного, системного и антивирусного программного обеспечения.

3.12. Ответственность за функциональность и работоспособность серверов почтовых систем возлагается на Оператора почтовой системы.

3.13. Ответственность за сохранность и конфиденциальность персональных идентификационных данных пользователей сервисом электронной почты возлагается персонально на каждого пользователя и уполномоченных сотрудников, осуществляющих их регистрацию.

ГЛАВА 4
ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Разграничение доступа сотрудников Академии образования к объектам информационной сети определено должностными инструкциями, приказом ректора от 19.06.2024 № 223 «Об использовании персональных данных» и дополнительно технически реализуется с помощью программного обеспечения, функционирующего на серверах Академии образования, принятых в Академии образования правил IP-адресации и политики использования учетных записей пользователей.

4.2. Сотрудники Академии образования имеют право:

пользоваться локальными сетевыми ресурсами и ресурсами глобальной компьютерной сети Интернет для выполнения своих должностных обязанностей;

использовать сервис электронной почты для выполнения своих должностных обязанностей;

информировать непосредственного руководителя структурного подразделения Академии образования по вопросам, возникающим при использовании сетевых ресурсов и сервисов;

вносить предложения по улучшению работы сети.

4.3. Сотрудники Академии образования обязаны:

соблюдать требования законодательства Республики Беларусь и настоящей Политики при работе с сетевыми информационными ресурсами;

использовать ресурсы и сервисы глобальной компьютерной сети Интернет только для выполнения служебных обязанностей;

в случае обнаружения вредоносных программ, нестандартного поведения пользовательских приложений, возникновении нештатных ситуаций в работе компьютерных систем немедленно информировать об этом непосредственного руководителя структурного подразделения Академии образования.

4.4. Сотрудникам Академии образования запрещается:

использовать глобальную компьютерную сеть Интернет на компьютерах, где хранится и обрабатывается конфиденциальная служебная информация;

использовать в информационной сети Академии образования личные мобильные технические средства;

подключаться к глобальной компьютерной сети Интернет, используя компьютер организации, через неслужебный канал доступа – мобильное устройство, модем и другие устройства;

допускать к работе за компьютером посторонних лиц;

при подключении к глобальной компьютерной сети Интернет обходить учетную систему, систему статистики, повреждать или дезинформировать их; осуществлять попытки несанкционированного доступа к ресурсам, проводить сетевые атаки и сетевой взлом или участвовать в них; использовать программные продукты, ресурсы глобальной компьютерной сети Интернет, предназначенные для сокрытия действий пользователей;

распространять в глобальной компьютерной сети Интернет непроверенные или заведомо ложные данные, информацию, унижающую честь и достоинство граждан, а также сведения служебного характера без разрешения руководителя;

устанавливать на компьютер программное обеспечение, принимать предложения по обновлению программного обеспечения из непроверенных ресурсов глобальной компьютерной сети Интернет без согласования с отделом компьютерного обеспечения и сетевого администрирования;

предоставлять иным лицам пароль доступа к своему почтовому ящику;

рассылать по электронной почте материалы, содержащие 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;

переходить по ссылкам и открывать письма с вложениями, полученными от неизвестных отправителей;

распространять информацию ограниченного доступа, предназначенную для служебного использования, в том числе сведения, составляющие персональные данные и иную конфиденциальную информацию.