

ПОЛИТИКА
информационной безопасности
в Государственном учреждении
образования «Академия
последипломного образования»

Политика информационной безопасности 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 Государственном учреждении образования «Академия последипломного образования» (далее – академия).

Настоящая Политика разработана в соответствии со следующими нормативными правовыми и иными актами:

Законом Республики Беларусь от 10 ноября 2008 г. № 455-3 «Об информации, информатизации и защите информации»;

Законом Республики Беларусь от 7 мая 2021 г. № 99-3 «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».

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Система информационной безопасности в академии как организованная совокупность специальных средств, методов и мероприятий, предназначена для:

прогнозирования, своевременного выявления и устранения угроз профессионально значимым ресурсам и информационным системам академии 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. Контроль за исполнением мероприятий по информационной безопасности в академии последипломного образования осуществляет проректор по учебной работе.

1.3. Сотрудники академии 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.

ГЛАВА 2

ОРГАНИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. В локальной сети академии созданы три изолированных сегмента:

сегмент локальной сети в пределах кабинетов сотрудников управления бухгалтерского учета и финансов, не имеющий подключений к открытым каналам передачи данных;

сегмент локальной сети компьютерных классов академии для обмена данными в образовательном процессе, подключенный к открытому каналу передачи данных;

сегмент локальной сети академии 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. В соответствии с приказом проректора по методической работе академии от 08.04.2022 № 44 «О создании комиссии по отнесению информационных систем академии к классу типовых информационных

систем» составлены акты отнесения информационных систем 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:

локальная система управления образовательным процессом в академии: планирование, регистрация и анкетирование слушателей, учет учебной нагрузки и т.п.;

программное обеспечение «ИС: Бюджет 7.7 Бухгалтерия»;

программное обеспечение «ИС: Бюджет 7.7 Зарплата и кадры»;

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:

официальный сайт Государственного учреждения образования «Академия последипломного образования» (регистрационный № 1180300253 от 15.09.2003 с изменениями от 11.08.2020 в Государственном регистре информационных ресурсов);

сайт библиотеки государственного учреждения образования «Академия последипломного образования» (регистрационный № 1180300252 от 15.09.2003 в Государственном регистре информационных ресурсов);

система дистанционного обучения Государственного учреждения образования «Академия последипломного образования» (регистрационный № 1141303644 от 06.11.2013 с изменениями от 11.08.2020 в Государственном регистре информационных ресурсов);

диагностика профессиональной компетентности воспитателя дошкольного образования (регистрационный № 1141918192 от 29.04.2019 с изменениями от 11.08.2020 в Государственном регистре информационных ресурсов).

2.3. Организация и обеспечение эффективности функционирования системы информационной безопасности в академии возлагаются на центр информационных технологий.

2.4. Начальник центра информационных технологий по согласованию с ректором и(или) проректором по учебной работе академии определяет основные положения сетевой политики и технологии ее реализации. Функции оперативного управления техническими ресурсами системы защиты информации возлагаются на специально

назначенных сотрудников центра информационных технологий (уполномоченных).

2.5. Уполномоченный сотрудник центра информационных технологий имеет право по согласованию с ректором и(или) проректором по учебной работе академии проводить специальные технические мероприятия для выявления попыток повреждения оборудования, взлома программного обеспечения и несанкционированного доступа к ресурсам локальной сети или глобальной компьютерной сети Интернет.

2.6. Уполномоченный сотрудник центра информационных технологий 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.

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

2.8. Ответственность за использование сетевых ресурсов в учебных аудиториях во время проведения учебных занятий несет преподаватель.

ГЛАВА 3

ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Внешний и VPN каналы передачи данных предоставляются академии 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 за строго определенными рабочими местами и идентифицируются в локальной сети на основании фиксированных IP-адресов.

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

3.4. Применение специализированного программного обеспечения доступа пользователей локальной сети в глобальной компьютерной сети Интернет разрешается только через внутренний контролируемый прокси-сервер академии.

3.5. Определен минимальный перечень разрешенного программного обеспечения и регламентирован порядок его установки и использования:

Microsoft Windows;

Microsoft Office;

Системы антивирусной защиты;

Система межведомственного документооборота (СМДО) – общий отдел;

«ИС: Бюджет 7.7 Бухгалтерия» – управление бухгалтерского учета и финансов;

«ИС: Бюджет 7.7 Зарплата и кадры» – управление бухгалтерского учета и финансов;

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

3.6. Обмен информацией между пользователями локальной сети осуществляется посредством сетевых дисков с настроенными правами доступа.

3.7. Доступ пользователей к ресурсам глобальной компьютерной сети Интернет регламентируется прокси-сервером. Это позволяет задавать

необходимые разрешения по скорости, объему трафика и времени доступа, устанавливать 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.

3.9. На серверах академии настроен 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 аутентификации.

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.

ГЛАВА 4

ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Разграничение доступа сотрудников академии к объектам информационной сети определено должностными инструкциями, приказом ректора академии от 23.11.2021 № 105 «Об использовании персональных данных» и дополнительно технически реализуется с помощью программного обеспечения серверов академии, политик IP-адресации и учетных записей пользователей.

4.2. Сотрудники академии имеют право:

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

обращаться за помощью в центр информационных технологий по вопросам, возникающим при использовании сетевых ресурсов и сервисов; вносить предложения по улучшению работы сети.

4.3. Сотрудники академии 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 сообщать об этом в центр информационных технологий.

4.4. Сотрудникам академии запрещается:

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

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 центром информационных технологий;

при использовании электронных почтовых ящиков открывать сообщения от непроверенных адресатов, осуществлять рассылку спама.