Министерство образования Московской области
Государственное бюджетное профессиональное образовательное учреждение Московской области «Щелковский колледж»
(ГБПОУ МО «Щелковский колледж»)

ПРИНЯТО

на заседании Совета колледжа
протокол № 9
от 05 сентября 2025г.

УТВЕРЖДАЮ

Директор ГБПОУ МО
«Щелковский колледж»

_____ Ф.В. Бубич

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 151C95EF0C4C9A9AC1B0C183E509994A
Владелец: Бубич Флора Владимировна
Действителен: с 05.03.2025 до 29.05.2026

ПОЛОЖЕНИЕ № 117

о доступе к информационным ресурсам

г.о.Щёлково, деревня Долгое Ледово
2025г.

1. Назначение и область действия

1.1. Настоящее Положение о доступе к информационным ресурсам (далее – Положение) определяет основные правила и требования по обеспечению ИБ информационных ресурсов Государственного бюджетного профессионального образовательного учреждения Московской области «Щелковский колледж» (далее – Колледж) от любых форм неавторизованного доступа, использования и раскрытия информации.

1.2. Соответствует требованиям Концепции и Политики ИБ Колледжа.

1.3. Распространяется на всех обучающихся, работников Колледжа и третьих лиц, использующих информационные ресурсы и системы Колледжа. Является обязательным для исполнения.

2. Основные требования

2.1. Получение пользователями доступа к информационным ресурсам основывается на аутентификации этих пользователей и разграничении доступа.

2.2. В качестве объектов доступа рассматриваются информационные ресурсы Колледжа, в отношении которых Колледж имеет права владения, распоряжения, пользования: данные (информация), технические средства, программные средства, услуги (сервисы) информационных систем.

2.3. Каждому пользователю сопоставляется учетная запись пользователя, присваиваются, по возможности, единые для различных объектов доступа Колледжа атрибуты ИБ: уникальный идентификатор, «секрет» аутентификации, права доступа – с учетом их важности и ценности для деятельности Колледжа.

2.4. В Колледже могут применяться виды аутентификации, основанные на знании пользователем пароля (базовый вид аутентификации), на владении физическим носителем «секрета» (смарт-карты, устройства контактной памяти, USB-ключи, криптографические токены), на уникальных данных пользователя (биометрические параметры). При необходимости может использоваться комбинация двух или более видов.

2.5. Пользователи уведомляются об обязанностях по обращению с «секретами» аутентификации и сроках истечения их действия. «Секреты», в свою очередь, передаются пользователям способом, исключающим несанкционированное ознакомление с ними. Передача пользователем личного «секрета» другому лицу запрещена.

2.6. Назначение прав доступа соответствует принципу «Запрещено все, что явно не разрешено» и определяется, исходя из служебных обязанностей пользователя.

2.7. Категорически запрещен доступ к ресурсам по принципу «Всем – Полный доступ». Запрещен также неавторизованный (анонимный, гостевой) доступ к любым ресурсам, кроме общедоступных страниц веб-сайтов Колледжа.

2.8. Пересмотр прав доступа осуществляется при возникновении производственной необходимости и документируется.

2.9. Управление доступом к сетевым информационным ресурсам и услугам производится, в том числе, путем разделения информационной телекоммуникационной системы Колледжа на отдельные логические и физические сетевые сегменты.

2.10. В Колледже должны использоваться средства контроля над соблюдением правил доступа к объектам доступа.

2.11. Служебный доступ к объектам доступа Колледжа, осуществляемый по внешним каналам связи, должен защищаться с применением механизмов аутентификации и криптографической защиты информации.

2.12. Доступ к общедоступным страницам веб-сайтов Колледжа не требует соблюдения требований пункта 2.11., достаточно обеспечить шифрование трафика.

2.13. Для снижения вероятности угроз несанкционированного доступа, необходимо минимизировать число устройств, имеющих легальные внешние IP-адреса

сети Интернет. Оборудование, имеющее легальные внешние IP-адреса сети Интернет, должно проверяться на наличие уязвимостей и автоматически получать обновления безопасности.

2.14. Объекты доступа Колледжа должны быть защищены от внешних угроз из сети Интернет и из локальной сети сетевыми брандмауэрами и штатными средствами защиты, входящими в состав операционной системы и приложений. Число открытых для доступа сервисов и ресурсов на этих объектах должно быть минимально необходимым.

2.15. В договорах с поставщиками информационно-технических услуг определяются требования по управлению доступом к этим услугам.

2.16. При увольнении работника обеспечивается невозможность его доступа к объектам доступа Колледжа.

2.17. При нарушении требований данного Положения доступ пользователя к информационным ресурсам может быть временно заблокирован ответственными до устранения нарушения.

2.18. Порядок работы с информационными ресурсами, содержащими сведения, отнесенные к государственной тайне либо к персональным данным, защита которых организуется в соответствии с требованиями законодательства РФ, определяется соответствующими внутренними документами Колледжа. Разработка и утверждение этих документов производится вне настоящего Положения.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех обучающихся, работников Колледжа и третьих лиц, использующих информационные ресурсы и системы Колледжа.

3.2. Ответственность за реализацию данного Положения возлагается на:

- руководителей структурных подразделений Колледжа;
- работников, ответственных за администрирование сегментов информационной телекоммуникационной системы Колледжа;
- работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации

	Должность	Фамилия и инициалы
Разработано	Главный специалист по защите информации	Ольховский В.А.
Согласовано	Зам.директора по безопасности	Маликов А.В.