



БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА – ЮГРЫ
«ЛАНГЕПАССКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

УТВЕРЖДАЮ
И.о. директора БУ «Лангепасский
политехнический колледж»
И.А. Тихонова
Приказ № 651-Р
«06» 10 2026 г.



ПОЛОЖЕНИЕ
О ЗАЩИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ
В БУ «ЛАНГЕПАССКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

г. Лангепас

1 Общие положения

1.1 Положение о защите информационных систем (далее – Положение) определяет цель, задачи, меры по защите информационных систем и распределение обязанностей участников информационных отношений в БУ «Лангепасский политехнический колледж» (далее-колледж).

1.2 Положение разработано в соответствии со следующими нормативными правовыми и иными документами:

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
 - Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
 - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
 - Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
 - приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
 - приказ Федеральной службы по техническому и экспортному контролю 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;
 - письмо Министерства просвещения Российской Федерации от 10.11.2025 № ИШ-2224/04 «О направлении методических рекомендаций по обеспечению государственных и муниципальных образовательных организаций оптимальным и безопасным доступом к государственным, муниципальным и иным информационным системам, информационно-телекоммуникационной сети «Интернет»;
 - Методической документ. Методика оценки угроз безопасности информации, утвержденный Федеральной службой по техническому и экспортному контролю 05.02.2021;
 - ГОСТ Р 50922-2006. Защита информации. Основные термины и определения;
 - ГОСТ Р 59547-2021 Защита информации. Мониторинг информационной безопасности. Общие положения.
- 1.3 Обеспечение защиты информационных систем в колледже строится на комплексном подходе, включающем:
- анализ угроз безопасности информации;

- внедрение правовых, организационных, физических и технических мер защиты;
- учет машинных носителей информации;
- мониторинг и реагирование на инциденты информационной безопасности;
- обеспечение восстановления информации;
- контроль состояния защищенности систем;
- персональную ответственность должностных лиц.

2 Термины и определения

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная система – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Мониторинг информационной безопасности – процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей.

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

3 Цель и задачи защиты информационных систем

3.1 Целью защиты информационных систем колледжа является обеспечение их устойчивого и безопасного функционирования, а также защита обрабатываемой в них информации от случайного или преднамеренного воздействия, способного причинить ущерб субъектам информационных отношений.

3.2 Для достижения указанной цели система защиты информационных систем должна обеспечивать:

- доступность – возможность авторизованных пользователей получать необходимую информацию в установленное время при штатном функционировании систем;
- целостность и аутентичность – сохранение информации в неизменном виде и подтверждение ее авторства при обработке, хранении и передаче;
- конфиденциальность – сохранение в тайне информации ограниченного доступа, обрабатываемой в информационных системах.

3.3 Основные задачи системы защиты информационных систем:

- своевременное выявление, оценка и прогнозирование угроз безопасности информации;
- оперативное реагирование на угрозы и инциденты;
- минимизация и локализация ущерба от нарушений безопасности;
- защита от несанкционированного доступа к информационным системам;
- разграничение доступа пользователей в соответствии с их полномочиями;
- обеспечение идентификации и аутентификации пользователей;
- защита программных средств от несанкционированной модификации и внедрения вредоносного кода;
- защита информации от утечки по техническим каналам.

4 Объекты защиты и субъекты доступа к информационным системам

4.1 Защите подлежат все информационные системы колледжа, независимо от их местонахождения, числящиеся на балансе или в оперативном управлении образовательной организации.

4.2 Основные объекты защиты информационных систем:

- информационные системы, предназначенные для обработки персональных данных, содержащие персональные данные обучающихся, их родителей (законных представителей), работников колледжа и иных лиц;
- информационные системы, содержащие служебную информацию ограниченного распространения (кадровые, бухгалтерские, финансовые и иные системы);
- автоматизированные системы управления образовательным процессом (электронные журналы, электронные дневники, системы дистанционного обучения, образовательные платформы);
- официальный сайт колледжа в информационно-телекоммуникационной сети «Интернет» и иные информационные ресурсы, используемые для предоставления государственных и муниципальных услуг в электронной форме;
- локальные вычислительные сети и сегменты сети передачи данных, включая беспроводные сети, обеспечивающие функционирование информационных систем;
- средства вычислительной и организационной техники, серверное оборудование, системы хранения данных, программно-аппаратные комплексы, используемые для обработки защищаемой информации;
- каналы связи и телекоммуникационное оборудование, предназначенные для передачи информации;
- системы электронного документооборота и делопроизводства.

4.2.1 В составе информационных систем защите подлежат следующие компоненты:

- информация (данные), содержащаяся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.)

- программно-аппаратные средства обработки и хранения информации (в том числе автоматизированные рабочие места, серверы, включая промышленные, средства отображения информации, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства));

- программные средства (в том числе системное и прикладное программное обеспечение (далее – ПО), включая серверы приложений, веб-приложений, системы управления базами данных, системы виртуализации);

- машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию;

- телекоммуникационное оборудование (в том числе программное обеспечение для управления телекоммуникационным оборудованием);

- средства защиты информации (в том числе программное обеспечение для централизованного администрирования средств защиты информации);

- привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними;

- обеспечивающие системы.

4.3 К особенностям защищаемых объектов колледжа относятся: распределенный характер инфраструктуры, высокая интенсивность потоков данных, требование непрерывности работы и разнородный состав пользователей.

4.4 Субъектами доступа к информационным системам являются:

- работники колледжа – лица, состоящие в трудовых отношениях с образовательной организацией, допущенные к работе в информационных системах в соответствии с их должностными (функциональными) обязанностями;

- обучающиеся – лица, осваивающие образовательные программы, имеющие доступ к информационным системам в объеме, необходимом для осуществления образовательного процесса;

- родители (законные представители) обучающихся – лица, имеющие доступ к информационным системам в объеме, необходимом для получения информации об успеваемости и образовательном процессе;

- представители органов государственной власти и местного самоуправления – лица, осуществляющие контрольные, надзорные и иные функции, имеющие доступ в пределах установленных полномочий;

- иные лица – лица, которым предоставлен доступ к информационным системам в соответствии с законодательством Российской Федерации, договорами и локальными нормативными актами

образовательной организации (в том числе представители организаций-партнеров, подрядчики, обслуживающий персонал).

4.5 Субъекты доступа не вправе совершать действия, направленные на нарушение штатного режима функционирования информационных систем, получение несанкционированного доступа к информации, содержащейся в информационных системах, а также на создание условий для совершения таких действий иными лицами.

5 Основные угрозы информационной безопасности

5.1 В целях организации эффективной системы защиты информационных систем в колледже осуществляется идентификация, анализ и классификация угроз информационной безопасности по следующим критериям: по источнику возникновения, по намеренности, по цели воздействия (на что направлена угроза), по расположению источника угрозы, по характеру воздействия, по способу реализации (Приложение 1).

5.2 В колледже осуществляется мониторинг информационной безопасности в целях своевременного выявления угроз безопасности информации, нарушений установленных требований к защите информации и инцидентов, влияющих на безопасность информационных систем.

6 Принципы и меры защиты информационных систем

6.1 Система защиты информации в колледже строится на следующих принципах:

- законность – все меры защиты информации осуществляются в соответствии с требованиями законодательства Российской Федерации;
- комплексность – применение правовых, организационных и технических мер защиты в совокупности;
- системность – учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности образовательной организации;
- непрерывность – постоянное функционирование системы защиты информации в течение всего времени обработки защищаемой информации;
- своевременность – упреждающий характер мер обеспечения информационной безопасности;
- разграничение доступа – предоставление доступа к информации только лицам, имеющим на это право в соответствии с их должностными (функциональными) обязанностями;
- минимизация полномочий – предоставление пользователям минимально необходимого объема прав доступа для выполнения их функций;
- персональная ответственность – возложение ответственности на каждого пользователя за сохранность информации и соблюдение требований информационной безопасности;

– гибкость системы информационной безопасности – способность к адаптации при изменении внешних и внутренних условий осуществления образовательной и иной деятельности образовательной организации, в том числе:

при изменении организационной структуры и штатного расписания образовательной организации;

при внедрении новых или модернизации существующих информационных систем;

при вводе в эксплуатацию новых технических средств и оборудования;

при изменении нормативных требований в области защиты информации;

при выявлении новых актуальных угроз и уязвимостей, влияющих на безопасность информационных систем.

6.2 Правовой основой обеспечения защиты информационных систем колледжа является совокупность действующих законодательных и иных нормативных правовых актов Российской Федерации, регулирующих:

– правила обращения с информацией, в том числе ограниченного доступа;

– права и обязанности участников информационных отношений при обработке, хранении и передаче информации;

– ответственность за нарушение установленных правил и требований в области защиты информации.

6.3 К организационным (административным) мерам защиты информационных систем относятся регламентные процедуры, направленные на:

– ограничение физического доступа к элементам информационных систем (пропускной режим, допуск в помещения);

– упорядочение доступа пользователей к информационным ресурсам в соответствии с их полномочиями;

– управление изменениями аппаратных и программных ресурсов на основе заявок пользователей;

– обеспечение физической целостности и контроль неизменности конфигурации средств вычислительной техники;

– обучение и разъяснительную работу с пользователями по вопросам информационной безопасности;

– распределение обязанностей и ответственности между участниками процесса обеспечения безопасности;

– регламентацию порядка обработки конфиденциальной информации;

– установление мер ответственности за нарушения установленных правил

6.4 Физические меры защиты информационных систем основаны на применении механических, электронных и электронно-механических устройств для создания препятствий на возможных путях доступа

нарушителей к элементам информационных систем и защищаемой информации. К таким мерам относятся: организация контролируемого доступа в помещения; системы охранной сигнализации и видеонаблюдения; защита технических средств от физического воздействия; системы контроля и управления доступом.

6.5 Технические меры защиты информационных систем основаны на использовании электронных устройств и специализированного программного обеспечения для выполнения функций защиты: идентификации и аутентификации пользователей; разграничения доступа к ресурсам; регистрации событий безопасности; криптографического закрытия информации; антивирусной защиты; фильтрации сетевого трафика; резервного копирования и восстановления данных, а также применения средств защиты от автоматизированных атак и социальной инженерии, в том числе с использованием технологий искусственного интеллекта.

6.6 При разработке и приобретении программного обеспечения, используемого в информационных системах колледжа, должны соблюдаться общие требования к созданию безопасного программного обеспечения, включая требования к содержанию и порядку выполнения работ, связанных с созданием безопасного программного обеспечения и устранением выявленных недостатков и уязвимостей.

6.7 Образовательная организация обеспечивает применение мер защиты информационных систем на всех этапах их жизненного цикла:

- проектирование – закладка требований безопасности на этапе проектирования системы;
- создание и ввод в эксплуатацию – внедрение мер защиты, тестирование защищенности, аттестация системы;
- эксплуатация – постоянный мониторинг, обновление средств защиты, управление уязвимостями, реагирование на инциденты;
- модернизация – пересмотр мер защиты при изменении архитектуры или состава системы;
- вывод из эксплуатации – безопасное уничтожение или передача данных и носителей информации.

6.8 Обеспечение защиты информационных систем образовательной организации осуществляется, в том числе, через реализацию трудовых функций работниками, для которых профессиональными стандартами предусмотрены требования к обеспечению информационной безопасности.

6.9 В целях эффективной организации защиты информационных систем образовательной организации осуществляется разграничение следующих направлений деятельности:

Защита информации. Меры защиты информации включают:

- установление порядка доступа к информации и разграничение прав пользователей;
- применение средств криптографической защиты информации при передаче данных по открытым каналам связи;

- обеспечение сохранности персональных данных и иной информации ограниченного доступа;
- соблюдение требований, установленных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Защита информационной системы – комплекс организационных и технических мер, направленных на обеспечение технической безопасности среды обработки информации, включая защиту серверов, сетевого оборудования, программного обеспечения и каналов связи от несанкционированного доступа, вредоносных воздействий, сбоев и отказов. Меры защиты информационной системы включают:

- применение сертифицированных средств антивирусной защиты;
- использование межсетевых экранов (файрволов) и систем обнаружения вторжений;
- организацию резервного копирования и восстановления данных;
- обеспечение физической защиты технических средств;
- соблюдение требований к безопасной разработке программного обеспечения;
- внедрение системы мониторинга информационной безопасности.

6.10 Меры защиты информации и меры защиты информационной системы реализуются в комплексе и являются взаимодополняющими. Недостаточная защищенность информационной системы ставит под угрозу сохранность обрабатываемой информации, а недостаточный контроль за обращением информации делает неэффективными технические средства защиты системы.

6.11 Детализация отдельных мер защиты информационных систем осуществляется в соответствующих инструкциях и регламентах образовательной организации (в том числе порядок парольной защиты, порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей, антивирусной защиты, обеспечения сохранности конфиденциальных документов, порядок предоставления пользователям доступа к информационным системам, в том числе удаленного, порядок предоставления пользователям доступа из информационных систем в телекоммуникационную сеть «Интернет» и контроля ее использования и др.).

7 Распределение обязанностей по защите информационных систем

7.1 Ответственность за организацию защиты информационных систем возлагается на директора колледжа, который:

- определяет уполномоченное лицо для координации работ в области защиты информационных систем;

– вводит в действие перечень должностей и лиц, допущенных к работе с информационными системами и содержащейся в них информацией, с указанием объема их полномочий.

7.2 Уполномоченное лицо (техник по защите информации) осуществляет:

- разработку и актуализацию внутренней нормативной и методической документации по вопросам защиты информационных систем;
- мониторинг исполнения требований вышестоящих органов и уполномоченных организаций в части защиты информации;
- организацию и контроль применения мер защиты в отношении информации, обрабатываемой в информационных системах;
- регулярную проверку состояния средств защиты и эффективности организационных мероприятий;
- проведение инструктажей с пользователями информационных систем по правилам безопасной работы;
- контроль за деятельностью техников-программистов в части поддержания работоспособности средств защиты, включая управление доступом, антивирусную защиту и резервное копирование;
- учет и контроль оборота носителей информации, содержащих сведения ограниченного доступа;
- согласование изменений в аппаратно-программной конфигурации информационных систем с точки зрения их влияния на безопасность;
- организацию контроля за техническим обслуживанием и ремонтом средств вычислительной техники, входящих в состав информационных систем;
- оперативное изменение учетных данных (паролей) при кадровых изменениях работников, имеющих доступ к системам;
- выдачу обязательных для исполнения предписаний об устранении выявленных нарушений;
- немедленное пресечение попыток несанкционированного доступа к информационным системам и информирование директора колледжа о таких фактах;
- подготовку отчетности о состоянии защиты информационных систем и информирование директора о выявленных недостатках.

7.3 Техники-программисты в рамках исполнения трудовых функций, предусмотренных их должностными инструкциями, осуществляют техническое сопровождение системы защиты.

7.4 Пользователи информационных систем (работники, обучающиеся, иные лица, имеющие доступ к системам) обязаны:

- руководствоваться требованиями настоящего Положения;
- использовать предоставленный доступ к информационным системам исключительно в целях выполнения своих трудовых (функциональных, образовательных) задач;

- незамедлительно информировать директора колледжа о любых обстоятельствах, создающих угрозу безопасности информационных систем (подозрительная активность, попытки несанкционированного доступа, утрата учетных данных);

- обеспечивать конфиденциальность своих учетных данных и не передавать их третьим лицам.

7.5 Техник по защите информации имеет право:

- запрашивать у пользователей необходимую информацию и документы по вопросам соблюдения требований защиты информационных систем;

- давать обязательные для исполнения указания в пределах своей компетенции;

- временно ограничивать доступ пользователей к информационным системам при выявлении нарушений, создающих угрозу безопасности;

- инициировать перед директором колледжа применение мер ответственности к лицам, допустившим нарушения.

8 Заключительные положения

8.1 Настоящее Положение вступает в силу с момента его утверждения и действует до его отмены или принятия нового положения.

8.2 Вопросы, не урегулированные настоящим Положением, решаются в соответствии с действующим законодательством Российской Федерации, Уставом и локальными нормативными актами образовательной организации.

Приложение 1

к Положению о защите информационных систем
образовательной организации среднего профессионального образования

Классификация основных угроз информационных систем

По источнику возникновения		
Категория	Описание	Примеры
Антропогенные	Связаны с действиями людей	Преднамеренные: хакерские атаки, промышленный шпионаж, саботаж; непреднамеренные: ошибки персонала, некомпетентность, халатность, случайное удаление файлов
Техногенные	Возникают из-за сбоев в технике и программном обеспечении	Ошибки в программном обеспечении, уязвимости, неправильная настройка систем, аппаратные сбои, отказы оборудования
Природные	Обусловлены стихийными бедствиями и внешними природными факторами	Пожары, наводнения, землетрясения, ураганы, молнии, перепады температуры, приводящие к физическому уничтожению оборудования и потере данных
По намеренности		
Преднамеренные (умышленные)	Целенаправленные действия злоумышленников	Взлом информационных систем, внедрение вредоносного ПО, фишинг, социальная инженерия, DDoS-атаки
Непреднамеренные (случайные)	Возникают из-за ошибок, халатности или стечения обстоятельств	Отправка конфиденциальных данных не тому адресату, сбой сервера из-за перегрева, воздействие физических полей других устройств, случайное уничтожение данных
По цели воздействия (на что направлена угроза)		
Нарушение конфиденциальности	Угрозы, направленные на	Кража баз данных, перехват трафика,

	несанкционированное получение информации ограниченного доступа	несанкционированный доступ, утечка персональных данных
Нарушение целостности	Угрозы, направленные на несанкционированное изменение, подмену или уничтожение данных	Внедрение вирусов, подмена документов, модификация баз данных, искажение информации
Нарушение доступности	Угрозы, направленные на блокирование или ограничение доступа к информации и ресурсам	DDoS-атаки (перегрузка сервера), программы-вымогатели (шифрование данных с требованием выкупа), вывод оборудования из строя
По расположению источника угрозы		
Внутренние	Исходят от лиц, имеющих легальный доступ к информационным системам образовательной организации	Сотрудники, подрядчики, партнеры; случайные ошибки или умышленные действия (кража клиентской базы перед увольнением, саботаж)
Внешние	Иницируются злоумышленниками извне	Хакеры, преступные группы, (в рамках кибершпионажа)
По характеру воздействия		
Активные	Нацелены на непосредственное нарушение работы информационной системы	Внедрение вредоносного кода, искажение данных, блокировка сервисов, удаление файлов
Пассивные	Характеризуются скрытым сбором информации без вмешательства в работу системы	Перехват трафика, анализ логов, сбор учетных данных с помощью шпионского ПО, прослушивание каналов связи
По способу реализации		
Технические	Используют уязвимости в программном обеспечении,	Эксплойты, вирусы, трояны, черви, SQL-инъекции, межсетевые атаки

	аппаратном обеспечении, сетях	
Социальные (социальная инженерия)	Манипулируют людьми для получения доступа к информации или системам	Фишинг (разновидность социальной инженерии, вид интернет-мошенничества, при котором злоумышленники обманом выманивают у людей конфиденциальные данные: логины и пароли от аккаунтов, реквизиты банковских карт, паспортные данные и другую личную информацию), вишинг (голосовой фишинг), претекстинг (метод социальной инженерии, при котором злоумышленник заранее придумывает вымышленный сценарий (претекст), чтобы установить доверительные отношения с жертвой и обманом заставить ее раскрыть конфиденциальную информацию, совершить определенные действия или предоставить доступ к ресурсам), плечевой серфинг (метод социальной инженерии, при котором злоумышленник тайно наблюдает за действиями жертвы, чтобы получить доступ к ее конфиденциальной информации: паролям, PIN-кодам, данным банковских карт, номерам социального страхования и другим личным сведениям), подделка документов

Физические	Связаны с непосредственным доступом к технике и оборудованию	Кража ноутбуков или жестких дисков, проникновение в серверную, уничтожение оборудования, несанкционированное подключение к сетям
------------	--	--