САНКТ-ПЕТЕРБУРГСКОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «АКАДЕМИЯ УПРАВЛЕНИЯ ГОРОДСКОЙ СРЕДОЙ, ГРАДОСТРОИТЕЛЬСТВА И ПЕЧАТИ»

(СПб ГБПОУ «АУГСГиП»)

П Р И К А З

19.03.2026 **№ 142/2**

Об утверждении Положения о Управлении информационных технологий и безопасности СПб ГБПОУ «АУГСГиП»

В соответствии с приказом от 01.02.2022 № 51 «Об утверждении требований к структуре и содержанию положения о структурном подразделении СПб ГБПОУ «АУГСГиП»

ПРИКАЗЫВАЮ:

1. Утвердить Положение о Управлении информационных технологий и безопасности СПб ГБПОУ «АУГСГиП» в новой редакции.
2. Начальнику Управления информационных технологий и безопасности Светличному В.И. разместить Положение на официальном сайте СПб ГБПОУ «АУГСГиП».
3. Контроль за исполнением настоящего приказа возложить на Пластун Олега Юрьевича.

Директор **А.М. Кривоносов**

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00F888BBB6190C0BBF783F46124F237295
Владелец: Кривоносов Анатолий Михайлович
Действителен: с 14.05.2025 до 07.08.2026

УТВЕРЖДЕНО
Приказом директора СПб ГБПОУ «Академии управления городской средой, градостроительства и печати»
от «___» _____ 20___ г. № ___

ПОЛОЖЕНИЕ
об Управлении информационных технологий и безопасности Академии управления городской средой, градостроительства и печати

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Управление информационных технологий и безопасности (далее — Управление) является самостоятельным структурным подразделением Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Академия управления городской средой, градостроительства и печати» (далее — Академия).

1.2. Управление создано в целях обеспечения бесперебойного функционирования информационно-технологической инфраструктуры Академии, технической поддержки образовательной и административной деятельности, а также обеспечения информационной безопасности.

1.3. Управление в своей деятельности руководствуется законодательством Российской Федерации, включая:

- Конституцию Российской Федерации;
- Федеральный закон № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон № 152-ФЗ «О персональных данных»;
- Федеральный закон № 63-ФЗ «Об электронной подписи»;
- Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Федеральный закон № 390-ФЗ «О безопасности»;

- нормативные правовые акты ФСТЭК России, ФСБ России, Минцифры России;
- Устав Академии; локальные нормативные акты Академии; настоящее Положение.

1.4. Управление подчиняется директору Академии либо заместителю директора в соответствии с распределением обязанностей, установленным приказом директора.

1.5. Структура и штатная численность Управления утверждаются директором Академии.

1.6. Управление возглавляет начальник Управления, назначаемый и освобождаемый от должности приказом директора Академии.

1.7. Настоящее Положение вступает в силу с момента его утверждения директором Академии.

2. ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ УПРАВЛЕНИЯ

2.1. Деятельность Управления направлена на:

а) исключение или существенное снижение негативных последствий (ущерба) в отношении Академии вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления в результате реализации угроз безопасности информации;

б) обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

в) повышение защищенности Академии от возможного нанесения ей материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем Академии или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;

г) обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры Академии;

д) обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры Академии.

2.2. Основными задачами деятельности Управления являются:

2.2.1. Обеспечение функционирования и развития информационно-технологической инфраструктуры Академии.

2.2.2. Организация и обеспечение информационной безопасности информационных систем и ресурсов Академии, включая контроль эффективности предусмотренных мер защиты информации.

2.2.3. Защита персональных данных работников, обучающихся и иных субъектов персональных данных.

2.2.4. Обеспечение функционирования информационных систем, используемых в образовательной и административной деятельности.

2.2.5. Развитие цифровой инфраструктуры Академии и внедрение современных информационных технологий.

2.2.6. Обеспечение приоритетного использования российского программного обеспечения, включённого в единый реестр российских программ для ЭВМ и баз данных (149-ФЗ, Постановление Правительства РФ № 1236, № 1875), и применения сертифицированных средств защиты информации (в соответствии с требованиями ФСТЭК России).

2.2.7. Организация резервного копирования данных и обеспечение восстановления информации при сбоях и инцидентах.

3. ФУНКЦИИ УПРАВЛЕНИЯ

Управление в соответствии с возложенными задачами выполняет следующие функции:

3.1. Техническое обслуживание и эксплуатация компьютерной техники, серверного оборудования, сетевой инфраструктуры и периферийных устройств Академии.

3.2. Администрирование локальных вычислительных сетей, серверных систем, систем хранения данных и информационных сервисов.

3.3. Установка, настройка и сопровождение программного обеспечения.

3.4. Ведение учета информационных ресурсов, программного обеспечения, лицензий и ИТ-активов Академии.

3.5. Техническая поддержка пользователей информационных систем.

3.6. Участие в подготовке технических заданий и документации при закупках ИТ-оборудования, программного обеспечения и услуг.

3.7. Сопровождение и развитие корпоративных информационных систем, систем электронного документооборота, образовательных платформ и иных цифровых сервисов.

3.8. Обеспечение защиты персональных данных:

3.8.1. Организация обработки персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.8.2. Реализация мер защиты персональных данных при их обработке в информационных системах персональных данных (ИСПДн), включая выполнение требований к защите ПДн, содержащихся в Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 235.

3.8.3. Проведение инвентаризации ИСПДн, определение их уровней защищённости, разработка и актуализация модели угроз.

3.8.4. Обеспечение прав субъектов персональных данных, ведение реестра ИСПДн, взаимодействие с Роскомнадзором.

3.9. Обеспечение информационной безопасности общего профиля:

3.9.1. Обеспечение защиты информации, не составляющей государственную тайну, в том числе сведений, составляющих коммерческую тайну и

служебную тайну, от утечки по техническим каналам, несанкционированного доступа и иных неправомерных действий.

3.9.2. Организация системы обнаружения и предотвращения компьютерных атак (СОВ), мониторинг информационной безопасности, реагирование на компьютерные инциденты.

3.9.3. Управление доступом к информационным ресурсам, обеспечение разграничения прав пользователей, защита информации при её передаче по каналам связи.

3.9.4. Проведение анализа защищённости информационных систем, оценка соответствия требованиям безопасности информации, утверждённым ФСТЭК России и ФСБ России.

3.10. Разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в Академии.

3.11. Разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в Академии и представление их директору Академии.

3.12. Выявление и проведение анализа угроз безопасности информации в отношении Академии, уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств и принятие мер по их устранению.

3.13. Обеспечение в соответствии с требованиями по информационной безопасности, в том числе с целью исключения (невозможности реализации) негативных последствий, разработки и реализации организационных мер и применения средств обеспечения информационной безопасности.

3.14. Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты.

3.15. Проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации)

основных процессов Академии в целях обеспечения информационной безопасности.

3.16. Организация развития навыков безопасного поведения в Академии, в том числе проведение занятий с руководящим составом и специалистами Академии по вопросам обеспечения информационной безопасности.

3.17. Планирование и реализация мероприятий по информационной безопасности, обеспечение методического руководства структурными подразделениями Академии при проведении работ по защите информации.

3.18. Мониторинг состояния информационной безопасности, выявление и реагирование на инциденты.

3.19. Организация резервного копирования информации и проведение тестирования восстановления данных.

3.20. Участие в организации и осуществлении мероприятий по профессиональной подготовке и переподготовке кадров Академии, проведении совещаний, семинаров по вопросам, входящим в компетенцию Управления.

3.21. Взаимодействие с органами исполнительной власти Санкт-Петербурга и Северо-Западного федерального округа, исполняющими контрольные функции по вопросам информационных технологий и информационной безопасности, в пределах своей компетенции.

3.22. Проведение внутренних проверок соблюдения требований информационной безопасности в структурных подразделениях Академии.

3.23. Формирование и ведение реестра информационных систем Академии, включая сведения об их назначении, владельцах систем, используемых программных и технических средствах.

3.24. Организация работ по определению уровня защищенности информационных систем персональных данных, категорированию информационных систем и разработке моделей угроз безопасности информации.

3.25. Участие в организации реагирования на компьютерные инциденты, связанные с нарушением функционирования информационных систем или угрозами информационной безопасности.

3.26. Формирование и реализация единой технической политики Академии в области использования информационных технологий, программного обеспечения и средств защиты информации.

3.27. Участие в согласовании закупок информационно-технологического оборудования, программного обеспечения и услуг в сфере информационных технологий для нужд Академии в целях обеспечения совместимости, безопасности и эффективности использования информационных ресурсов.

3.28. Организация централизованного управления учетными записями, правами доступа пользователей информационных систем Академии, включая создание, изменение, блокирование и удаление учетных записей.

3.29. Участие в согласовании внедрения и подключения новых информационных систем, сервисов и программного обеспечения в информационную инфраструктуру Академии.

3.30. Проведение анализа и аудита состояния информационно-технологической инфраструктуры и информационной безопасности в структурных подразделениях Академии.

3.31. Координация деятельности структурных подразделений Академии по вопросам информационной безопасности и защиты информации.

3.32. Участие в проведении служебных проверок по фактам нарушений информационной безопасности и инцидентов, связанных с использованием информационных систем Академии.

3.33. Инициирование приостановления эксплуатации информационных систем, программного обеспечения или технических средств, использование которых создает угрозу информационной безопасности либо нарушает требования законодательства Российской Федерации.

3.34. Обеспечение информационной безопасности при применении средств криптографической защиты информации и электронных подписей, ведение

их учета установленным порядком. Организация использования усиленных квалифицированных электронных подписей работниками Управления в целях подписания служебной документации, договоров, отчетности и иных документов в рамках компетенции Управления.

3.35. Формирование и представление отчетности в области информационной безопасности и защиты персональных данных, включая:

- отчеты о состоянии защищенности информационных систем и персональных данных в уполномоченные органы (Роскомнадзор, ФСТЭК России, ФСБ России) в сроки и по формам, установленным законодательством Российской Федерации;
- внутреннюю отчетность руководству Академии о состоянии информационной безопасности, выполнении плана мероприятий по защите информации и персональных данных;
- отчетность в информационные системы в сфере образования (включая СПО, КНВШ и иные федеральные информационные системы) в порядке и сроки, установленные нормативными правовыми актами и методическими рекомендациями. Перечень, формы и сроки представления отчетности определяются локальными нормативными актами Академии и требованиями уполномоченных органов.

3.36. Выполнение иных функций, исходя из поставленных руководством Академии целей и задач в рамках обеспечения информационной безопасности в Академии.

4. ПРАВА УПРАВЛЕНИЯ

4.1. Управление в пределах своей компетенции имеет право:

4.1.1. Запрашивать у структурных подразделений Академии документы, информацию и материалы, необходимые для выполнения своих функций.

4.1.2. Вносить руководству Академии предложения по развитию информационной инфраструктуры и совершенствованию информационной безопасности.

4.1.3. Участвовать в подготовке локальных нормативных актов Академии по вопросам информационных технологий и информационной безопасности.

4.1.4. Проводить проверки соблюдения требований информационной безопасности в подразделениях Академии.

4.1.5. Требовать от работников Академии соблюдения установленных правил использования информационных систем и средств вычислительной техники.

4.1.6. Временно ограничивать или блокировать доступ пользователей к информационным системам Академии в случаях выявления нарушений требований информационной безопасности либо угроз безопасности информации и уведомления пользователя/руководства при блокировке доступа и сроках такого ограничения.

4.1.7. Взаимодействовать с организациями и государственными органами по вопросам, входящим в компетенцию Управления.

4.1.8. Направлять сотрудников Управления на повышение квалификации.

4.1.9. Привлекать в установленном порядке специалистов научно-исследовательских и иных организаций, готовить материалы для заключения договоров с организациями на проведение и выполнение работ по вопросам, относящимся к компетенции Управления.

4.1.10. Контролировать деятельность структурных подразделений Академии в части выполнения ими требований по защите информации.

4.1.11. Использовать усиленную квалифицированную электронную подпись при подписании документов в пределах компетенции Управления.

4.1.12. Осуществлять иные права, предусмотренные законодательством Российской Федерации, законодательством субъекта Российской Федерации, нормативными правовыми актами представительных органов местного самоуправления.

5. ОТВЕТСТВЕННОСТЬ

5.1. Начальник Управления несёт ответственность за:

- организацию деятельности Управления;

- координацию выполнения возложенных на Управление задач и функций;
- обеспечение в пределах компетенции Управления соблюдения требований законодательства Российской Федерации в области информационных технологий, защиты информации и персональных данных;
- рациональное использование материальных и технических ресурсов, закреплённых за Управлением;
- своевременное и достоверное формирование отчетности в области информационной безопасности и защиты персональных данных.

5.2. Работники Управления несут ответственность за выполнение своих должностных обязанностей в соответствии с трудовым законодательством Российской Федерации и должностными инструкциями.

6. СТРУКТУРА И ОРГАНИЗАЦИЯ РАБОТЫ

6.1. В структуру Управления могут входить отделы (сектора) технической поддержки, сетевой инфраструктуры, информационных систем, информационной безопасности и иные подразделения.

6.2. Структура и штатное расписание Управления утверждаются директором Академии.

6.3. Начальник Управления:

6.3.1. Руководит деятельностью Управления и организует его работу.

6.3.2. Распределяет обязанности между работниками Управления.

6.3.3. Подписывает служебную документацию в пределах своей компетенции.

6.3.4. Представляет интересы Управления во взаимодействии со структурными подразделениями Академии и внешними организациями.

6.3.5. Вносит руководству Академии предложения о поощрении работников Управления либо привлечении их к дисциплинарной ответственности.

6.3.6. В пределах своей компетенции издает служебные распоряжения, указания и инструкции, обязательные для исполнения работниками Управления.

6.3.7. Дает обязательные для исполнения указания пользователям информационных систем Академии по вопросам эксплуатации информационных систем и соблюдения требований информационной безопасности.

6.3.8. Организует контроль соблюдения правил использования информационных систем Академии.

6.3.9. Организует использование усиленной квалифицированной электронной подписи работниками Управления в пределах их должностных обязанностей.

7. ВЗАИМОДЕЙСТВИЕ

7.1. Управление взаимодействует со всеми структурными подразделениями Академии по вопросам, относящимся к его компетенции.

7.2. Управление взаимодействует с государственными органами, организациями и поставщиками услуг в сфере информационных технологий и информационной безопасности.

8. ИМУЩЕСТВО

8.1. За Управлением закрепляется оборудование, программное обеспечение и иные материальные ресурсы, необходимые для выполнения его функций.

8.2. Работники Управления обязаны обеспечивать сохранность закрепленного имущества.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящее Положение утверждается приказом директора Академии.

9.2. Изменения и дополнения в настоящее Положение вносятся приказом директора Академии.

9.3. Положение подлежит пересмотру при изменении законодательства Российской Федерации, структуры Академии либо задач Управления.

9.4. Работники Управления, а также иные сотрудники Академии, деятельность которых связана с использованием информационных систем и

информационно-технологической инфраструктуры, знакомятся с настоящим Положением в установленном порядке.

9.5. Требования настоящего Положения являются обязательными для исполнения работниками Академии в части, касающейся использования информационных систем, средств вычислительной техники и соблюдения требований информационной безопасности.

9.6. Настоящее Положение вводится в действие с даты издания приказа директора Академии об его утверждении (или с даты, указанной в приказе).