Положение об Отделе информационной безопасности Управления проректора по цифровизации Томского политехнического университета

08.07.

УТВЕРЖДАЮ

Проректор по цифровизации
_____ К.Г. Квасников
«20» 08 2025 г.

1. Общие положения

1.1. Настоящее положение определяет цели, задачи и функции отдела информационной безопасности (сокращенное наименование – ОИБ), который является структурным подразделением Управления проректора по цифровизации федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский политехнический университет» (далее – Университет, ТПУ), являющегося субъектом критической информационной инфраструктуры Российской Федерации, обеспечивающим информационную безопасность Университета.

1.2. ОИБ создан в соответствии с приказом ректора Университета № 316-1/од от 12.11.2021.

1.3. В своей деятельности ОИБ руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, нормативными правовыми актами Министерства науки и высшего образования Российской Федерации и других федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности; другими нормативными правовыми документами в сфере обеспечения информационной безопасности, указаниями руководства Университета, Уставом Университета, локальными нормативными актами Университета, настоящим Положением.

1.4. ОИБ может быть реорганизован или его деятельность прекращена на основании приказа ректора Университета.

1.5. При реорганизации или прекращении деятельности ОИБ настоящее Положение утрачивает силу.

1.6. Изменения и дополнения настоящего Положения утверждаются проректором по цифровизации.

2. Структура и организация

2.1. ОИБ находится в оперативном подчинении проректора по цифровизации, ответственного за обеспечение информационной безопасности в Университете, который осуществляет контроль за деятельностью ОИБ.

2.2. Непосредственное руководство ОИБ осуществляет начальник отдела, который принимается на должность в соответствии с трудовым законодательством Российской Федерации в установленном порядке.

Дата актуализации: 20.08.2025
Разработчик: Ю.А. Ткаченко

2.3. Начальник ОИБ отвечает за организацию работы ОИБ, в том числе за соблюдение правил внутреннего трудового распорядка и охраны труда работниками ОИБ, за контролем над выполнением обязанностей, возложенных на подчиненных ему работников, сохранность имущества Университета, переданного ОИБ для выполнения его функций

2.4. ОИБ входит в состав Управления проректора по цифровизации, своего внутреннего деления не имеет.

3. Цели и задачи

Деятельность ОИБ направлена:

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

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

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

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

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

Основными задачами ОИБ являются:

3.1. Разработка и реализация единой политики информационной безопасности Университета.

3.2. Организация и обеспечение комплексной защиты информации в соответствии с политикой информационной безопасности Университета.

3.3. Планирование, организация и координация работ по обеспечению информационной безопасности и контроль за её состоянием в Университете.

3.4. Выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств (совместно с подразделением Управления проректора по цифровизации, ответственным за конкретный сегмент ИТ-инфраструктуры).

3.5. Предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию

(носители информации) в целях её добывания, уничтожения, искажения и блокирования доступа к ней.

3.6. Поддержание стабильной деятельности Университета и его производственных процессов в случае проведения компьютерных атак.

3.7. Взаимодействие с Национальным координационным центром по компьютерным инцидентам.

3.8. Нормативно-правовое обеспечение использования информационных ресурсов и процессов обеспечения информационной безопасности.

4. Функции

Для решения возложенных на ОИБ задач предусмотрено выполнение следующих функций:

4.1. Разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в Университете и его структурных подразделениях (за исключением Юргинского технологического института (филиала) ТПУ.

4.2. Разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в Университете и представление их проректору по цифровизации.

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

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

4.5. Обнаружение, предупреждение и ликвидация последствий компьютерных атак, и реагирование на компьютерные инциденты (совместно с подразделением Управления проректора по цифровизации, ответственным за конкретный сегмент ИТ-инфраструктуры).

4.6. Представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах (в координации с подразделением Управления проректора по цифровизации, ответственным за конкретный сегмент ИТ-инфраструктуры).

4.7. Организация работы по защите персональных данных в информационных системах Университета.

4.8. Организация и сопровождение средств криптографической защиты информации, их учет в Университете.

4.9. Организация защиты информационной безопасности объектов критической информационной инфраструктуры Университета.

4.10. Организация работы по защите информационных систем Университета (совместно с подразделением Управления проректора по цифровизации, ответственным за конкретный сегмент ИТ-инфраструктуры).

4.11. Разработка моделей угроз и нарушителя.

4.12. Осуществление мониторинга информационной безопасности, выявление, реагирование и ликвидация последствий инцидентов информационной безопасности (совместно с подразделением Управления проректора по цифровизации, ответственным за конкретный сегмент ИТ-инфраструктуры).

4.13. Организация проверок и разбирательств по инцидентам информационной безопасности.

4.14. Исполнение указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих Университету, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет".

4.15. Проведение анализа и контроль состояния защищенности систем и сетей, разработка предложений по модернизации (трансформации) основных процессов Университета в целях обеспечения информационной безопасности.

4.16. Подготовка отчетов о состоянии работ по обеспечению информационной безопасности в Университете.

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

4.18. Разработка локально-нормативных актов по обеспечению информационной безопасности.

4.19. Контроль исполнения основных положений Политики информационной безопасности Университета.

4.20. Выполнение иных функций, исходя из поставленных руководством Университета целей и задач в рамках обеспечения информационной безопасности в Университете.

5. Права подразделения

С целью реализации функций подразделение имеет право:

5.1. запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений органа (организации), необходимым для принятия решений по всем вопросам, отнесенным к компетенции подразделения;

5.2. готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности;

5.3. контролировать деятельность любого структурного подразделения Университета по выполнению требований к обеспечению информационной

безопасности;

5.4. постоянно повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности;

5.5. участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

5.6. участвовать в работе комиссий Университета при рассмотрении вопросов обеспечения информационной безопасности;

5.7. вносить предложения руководству Университета о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;

5.8. вносить представления руководству Университета в отношении работников Университета (далее - работники) при обнаружении фактов нарушения работниками установленных требований безопасности информации в Университете, в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности;

5.9. вносить на рассмотрение руководству Университета предложения по вопросам деятельности подразделения.

6. Взаимоотношения и связи подразделения

6.1. ОИБ осуществляет свои полномочия во взаимодействии со структурными подразделениями Университета, а также в пределах своей компетенции с иными организациями и гражданами в установленном порядке.

6.2. По указанию руководства осуществляет взаимодействие с Федеральной службой безопасности Российской Федерации, Национальным координационным центром по компьютерным инцидентам, Федеральной службой по техническому и экспортному контролю, Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций по вопросам информационной безопасности.

7. Показатели эффективности и результативности подразделения

7.1. Эффективность и результативность деятельности ОИБ определяются по итогам выполнения Университетом программы обеспечения информационной безопасности с учетом приоритетных целей, предусмотренных разделом 3 настоящего положения.

7.2. Работники ОИБ несут ответственность за выполнение возложенных на них обязанностей в соответствии с должностными регламентами, утверждаемыми проректором по цифровизации, наделенным соответствующими полномочиями.

8. Организация работы

8.1. Рабочее время работников ОИБ регулируется коллективным договором, правилами внутреннего трудового распорядка Университета, иными локальными нормативными актами.

8.2. Заработная плата работников ОИБ зависит от их квалификации, сложности выполняемой работы, количества и качества затраченного труда и устанавливается в соответствии со штатным расписанием ОИБ. В целях поощрения за достигнутые работниками успехи в работе и стимулирования дальнейшего их профессионального роста работникам ОИБ устанавливаются стимулирующие выплаты в соответствии с коллективным договором Университета.

9. Нормативные документы

9.1. Трудовой кодекс Российской Федерации;

9.2. нормативные правовые акты, регламентирующие деятельность, предусмотренную Уставом Университета;

9.3. Федеральный закон Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности»;

9.4. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

9.5. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

9.6. Федеральный закон Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

9.7. Федеральный закон Российской Федерации от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры РФ»;

9.8. нормативные и нормативно - методические акты Правительства Российской Федерации в области информационной безопасности;

9.9. нормативные и методические документы Федеральной службы по техническому и экспортному контролю Российской Федерации в области информационной безопасности;

9.10. нормативные и методические документы Федеральной службы безопасности Российской Федерации в области информационной безопасности;

9.11. нормативные и методические документы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в области информационной безопасности;

9.12. Устав Университета;

9.13. локальные нормативные акты Университета;

9.14. приказы и распоряжения ректора и администрации Университета;

9.15. коллективный договор Университета.