МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГТУ», ВГТУ)

УТВЕРЖДАЮ
Ректор ВГТУ
_____ Д.К. Проскурин
«_6_» _____ 2025 г.

Система менеджмента качества

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВГТУ

Воронеж 2025

1 РАЗРАБОТАНО рабочей группой

2 ОТВЕТСТВЕННЫЙ ИСПОЛНИТЕЛЬ проректор по цифровому развитию Бурковский А.В.

3 УТВЕРЖДЕНА И ВВЕДЕНА В ДЕЙСТВИЕ приказом от 06.05.2025 №01-1-08/294

4 ВВОДИТСЯ ВПЕРВЫЕ

1 Общие положения

1.1 Настоящий документ определяет политику федерального государственного бюджетного образовательного учреждения высшего образования «Воронежский государственный технический университет» в отношении информационной безопасности.

1.2 Политика информационной безопасности ВГТУ (далее – Политика) – это комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в ВГТУ для обеспечения информационной безопасности (далее – ИБ).

1.3 Настоящая Политика разработана в соответствии со следующими нормативно-правовыми актами:

- Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных».

1.4 В настоящей Политике используются следующие термины:

аутентификация: Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

защита информации: Деятельность университета по принятию правовых, организационных и технических мер направленных на защиту информации от неправомерного доступа.

информация: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

информационная безопасность: Практика предотвращения несанкционированного доступа (далее – НСД), использования, раскрытия, искажения информационных ресурсов университета.

инцидент информационной безопасности: Одно или серия нежелательных, или неожиданных событий ИБ, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу ИБ.

конфиденциальная информация: Информация с ограниченным доступом или ПДн, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

информационная система персональных данных: Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.5 Требования настоящей Политики распространяются на все структурные подразделения ВГТУ и обязательны к исполнению всеми работниками.

Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах ВГТУ, а также в договорах.

2 Цели и задачи Политики

2.1 Основными целями защиты информации в ВГТУ являются:

2.1.1 повышение стабильности функционирования университета в целом;

2.1.2 сохранение конфиденциальности информационных ресурсов;

2.1.3 обеспечение непрерывности доступа к информационным ресурсам;

2.1.4 достижение адекватности мер по защите от реальных угроз ИБ;

2.1.5 предотвращение или снижение ущерба от инцидентов ИБ.

2.2 Основными задачами деятельности по обеспечению ИБ являются:

2.2.1 контроль выполнения установленных требований по обеспечению ИБ;

2.2.2 повышение эффективности мероприятий по обеспечению и поддержанию ИБ с учетом законодательных требований;

2.2.3 разработка и совершенствование регламентирующих документов ВГТУ в области обеспечения ИБ;

2.2.4 выявление, оценка и прогнозирование угроз ИБ;

2.2.5 выработка рекомендаций по устранению уязвимостей;

2.2.6 организация антивирусной защиты информационных систем;

2.2.7 защита информации от НСД и утечки по техническим каналам связи.

3 Основные принципы обеспечения безопасности

Основными принципами обеспечения ИБ являются следующие:

3.1 анализ информационных систем с целью выявления их уязвимостей;

3.2 своевременное обнаружение проблем, потенциально способных повлиять на ИБ, корректировка моделей угроз и нарушителя;

3.3 разработка и внедрение защитных мер, адекватных характеру выявленных угроз;

3.4 контроль эффективности принимаемых защитных мер;

3.5 персонификация, разделение ролей и ответственности между работниками, исходя из принципа персональной ответственности за совершаемые операции.

4 Требования по обеспечению информационной безопасности

4.1 Комплекс мер по обеспечению ИБ предусматривает:

4.1.1 защиту информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации документов;

4.1.2 минимально необходимый, гарантированный доступ работника университета только к тем ресурсам информационного технологического

процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки информации;

4.1.3 контроль исполнения установленной технологии подготовки, обработки, передачи и хранения информации;

4.1.4 аутентификацию обрабатываемой информации;

4.1.5 восстановление информации в случае ее умышленного или случайного разрушения (искажения) или выхода из строя средств вычислительной техники;

4.1.6 гарантированную доставку сообщений участникам информационного обмена.

4.2 Требования по обеспечению ИБ на всех стадиях жизненного цикла информационных систем ВГТУ

4.2.1 Информационная безопасность должна обеспечиваться на всех стадиях технологических процессов, с учетом всех сторон, вовлеченных в процессы жизненного цикла.

4.2.2 Ввод в эксплуатацию и снятие с эксплуатации систем защиты осуществляются при участии работников, ответственных за обеспечение информационной безопасности.

4.2.3 Все объекты, критичные с точки зрения ИБ, т.е. сервера, маршрутизаторы и другие электронные устройства, находятся в охраняемых и контролируемых помещениях.

4.3 Требования по обеспечению ИБ при управлении доступом и регистрации

4.3.1 Все работы, связанные с обработкой и передачей информации, выполняются в соответствии с должностными обязанностями работников.

4.3.2 Работники ВГТУ, а также лица, принимаемые на работу по договорам гражданско-правового характера, допущенные к работе с конфиденциальной информацией, подписывают обязательство о неразглашении конфиденциальной информации;

4.3.3 Права доступа работников к персональным данным, устанавливаются в соответствии с Политикой в отношении обработки персональных данных и Положением об обработке персональных данных.

4.3.4 При обработке конфиденциальной информации в составе информационных систем, требуется использовать сертифицированные или разрешенные к применению средства защиты информации от НСД.

4.3.5 Авторизация, контроль и управление доступом к информационным активам, в том числе функционирование системы парольной защиты, осуществляются в соответствии с требованиями нормативных документов по организации парольной защиты.

4.3.6 Регистрация событий информационной системы производится в журналах событий системного программного обеспечения.

4.3.7 При взаимодействии с внешними информационными сетями используются защищенные каналы связи.

4.4 Требования по обеспечению ИБ при работе в локальной сети ВГТУ

4.4.1 Доступ работников к работе в информационных системах осуществляется в соответствии с их должностными обязанностями.

Регистрация выполняется системным администратором в соответствии с правами доступа работников ВГТУ к внутренним и внешним электронным информационным ресурсам.

Мониторинг информационной безопасности автоматизированных систем от НСД, распространения, искажения и утраты информации, осуществляет управление информационных технологий.

Предупреждение и своевременное выявление попыток НСД осуществляется с использованием средств операционной системы и специальных программных средств.

4.4.2 Требования к пользователям:

- при работе не использовать без необходимости потенциально опасные ресурсы сети Интернет (социальные сети, сторонние мессенджеры и т.п.);
- не устанавливать самостоятельно на компьютеры программное обеспечение и приложения, позволяющие осуществлять удаленный доступ к этому компьютеру;
- при работе с электронной почтой не открывать письма и вложения к ним, поступившие от неизвестных отправителей;
- исключить возможность установки посторонними лицами на компьютер вредоносного программного обеспечения.

На рабочих местах пользователей устанавливается антивирусное программное обеспечение с регулярным обновлением баз.

4.4.3 Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей.

При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учетными данными.

4.4.4 Ответственность за все действия в сети, произведенные под учетной записью пользователя, полностью лежит на самом пользователе. ВГТУ не несет никакой юридической, материальной или иной ответственности за качество, содержание, законность и любое другое свойство полученной или переданной пользователем информации в нарушение нас роящих требований.

4.5 Требования по обеспечению ИБ в сети Интернет

Руководство ВГТУ оставляет за собой право в целях обеспечения ИБ производить выборочные и полные проверки всей системы и отдельных файлов без предварительного уведомления работников и обучающихся.

4.5.1 Пользователям запрещается:

- посещение ресурсов, нарушающих нормы законодательства Российской Федерации;
- совершение действий, создающих чрезмерную нагрузку на оборудование сети и мешающих нормальной работе остальных пользователей;
- передача конфиденциальной информации третьим лицам;
- использование при работе учетных данных, принадлежащих другому пользователю;
- действия, направленные на причинение ущерба ВГТУ;
- попытки деструктивных действий в отношении третьих лиц (рассылка вирусов, интернет-атаки и т, п.);
- нарушение закона об авторском праве: копирование и использование материалов и программ, защищенных законом об авторском праве;
- несанкционированная рассылка электронных писем рекламного, коммерческого агитационного характера;
- осуществление попыток несанкционированного доступа к ресурсам сети, проведение или участие в сетевых атаках и сетевом взломе;
- совершение действий, противоречащих законодательству Российской Федерации, а также требованиям настоящей Политики.

4.5.2 Пользователи информационных ресурсов ВГТУ, нарушающие данные требования, могут быть отстранены от их использования, а также могут быть привлечены к административной ответственности.