

Федеральное государственное
бюджетное образовательное
учреждение высшего образования
«Воронежский государственный
университет»

УТВЕРЖДАЮ

Ректор ФГБОУ ВО «ВГУ»

Д.А. Ендовицкий

М.П.

«13» сентября 2016 г.



**ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

1. Общие положения и цели

1.1. Федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет» (далее - Университет) является унитарной некоммерческой организацией, созданной для осуществления образовательных, научных, социальных и культурных функций. Осуществление указанной деятельности связано с обработкой информации и зависит от обеспечения информационной безопасности, под которой понимается обеспечение конфиденциальности, целостности и доступности информационных активов.

1.2. Политика информационной безопасности (далее - Политика) устанавливает цели, задачи и подходы в области информационной безопасности, которыми Университет руководствуется в своей деятельности.

1.3. Политика направлена на достижение следующих целей:

- обеспечение непрерывности основных бизнес-процессов Университета;
- минимизация возможных потерь и ущерба от нарушений в области информационной безопасности.

2. Управление информационной безопасностью

2.1. Для достижения указанных целей в Университете внедряется система

управления информационной безопасностью (далее – СУИБ), которая соответствует требованиям законодательства Российской Федерации, нормативным и правовым документам Университета в области управления информационным обеспечением.

2.2. СУИБ Университета документирована в настоящей Политике, в распоряжениях, положениях, правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех работников Университета. Документированные требования СУИБ доводятся до сведения работников Университета.

2.3. Все информационные активы Университета, включая аппаратное обеспечение, программное обеспечение, информационные ресурсы на бумажных и электронных носителях подлежат учету и категорированию в соответствии с их важностью и степенью доступа.

2.4. Регулярное проведение оценки рисков информационной безопасности позволяет рассчитать вероятность возникновения угроз информационной безопасности и степень их влияния на бизнес-процессы, репутацию и финансовые активы Университета. По результатам оценки выбираются и применяются средства защиты информации физического, программного, аппаратного и организационного характера.

2.5. Университет стремится выявлять, учитывать и реагировать на инциденты в сфере информационной безопасности в соответствии с установленными процедурами. Для минимизации ущерба разрабатываются критерии контроля работы СУИБ, процедуры резервного копирования и восстановления информации.

2.6. Работники Университета получают доступ только к той информации, которая требуется для исполнения их функциональных обязанностей в рамках должностных полномочий. Университет проводит информирование и обучение работников в сфере информационной безопасности.

3. Ответственность

3.1. Руководство Университета осуществляет общее управление информационной безопасностью Университета и обеспечивает необходимые условия для:

- реализации мероприятий по оценке рисков информационной безопасности и защиты информации;

- поддержания, мониторинга, анализа и непрерывного улучшения системы управления информационной безопасностью;
- регулярного обучения работников Университета в сфере информационной безопасности.

3.2. Работники Университета несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех подозрениях и выявленных нарушениях в области информационной безопасности в Управление информатизации и компьютерных технологий Университета.

3.3. В должностных инструкциях работников Университета устанавливается ответственность за сохранность и конфиденциальность информации, ставшей известной работнику в силу выполнения своих обязанностей.


4. Заключительные положения

4.1. Руководство Университета утверждает настоящую Политику, которая внедрена и поддерживается в Университете.

4.2. Политика информационной безопасности Университета является общедоступным документом и размещается на официальном веб-сайте Университета www.vsu.ru.

РАЗРАБОТАНО – управлением информатизации и компьютерных технологий

ОТВЕТСТВЕННЫЙ ИСПОЛНИТЕЛЬ:
Начальник управления информатизации
и компьютерных технологий



А.Н. Прохорченко