МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»

ПРИКАЗ

«24» 10 2025 г. № 1803

Об утверждении плана мероприятий по защите информации, обрабатываемой в информационных системах персональных данных

В целях выполнения требований Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 №1119

ПРИКАЗЫВАЮ:

1. Утвердить план мероприятий по защите информации (Приложение), обрабатываемой в информационных системах персональных данных (далее – План).

2. Начальнику отдела информационной безопасности Линдигрин А.Н.:

- обеспечить выполнение утвержденного Плана в установленные сроки;
- обеспечить внесение изменений в План в случае изменения технологических процессов, структуры информационных систем персональных данных или требований законодательства.

3. Контроль за исполнением приказа возложить на проректора по общим вопросам и цифровизации Григорьева В. И.

Ректор О.А. Кравченко

И.о. ректора
А.А. Маликов

ЛИСТ СОГЛАСОВАНИЯ (ВИЗИРОВАНИЯ)

№ проекта: 2190-пр от 23.10.2025 Группа документов: Приказ по основной деятельности

Версия проекта: 1 Состав: 5

Содержание:

Об утверждении плана мероприятий по защите информации, обрабатываемой в информационных системах персональных данных

Исполнитель: Линдигрин А.Н. - начальник ОИБ;

ФИО и должность	Виза	Дата	Подпись	Примечание
Линдигрин А.Н. - начальник ОИБ (Отдел информационной безопасности (ОИБ))	Проект внесен	23.10.2025 09:59		
Колушкин С.А. - Начальник управления цифровизации (УЦ) (Управление цифровизации (УЦ))	Согласен	23.10.2025 16:55	Электронная подпись Сертификат: 116E9365C0671A3D34EE6A7441B25049 Кем выдан: uc_fk@roskazna.ru, 77 Москва, 7710568760, 1047797019830, Большой Златоустинский переулок, д. 6, строение 1, г. Москва, RU, Казначейство России, Федеральное казначейство Кому выдан: RU, Тульская область, начальник управления, Управление цифровизации, ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ТУЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", 03434081318, 710601133402, oib@tsu.tula.ru, Сергей Александрович, Колушкин, Колушкин Сергей Александрович Действителен: с 09.07.2025 8:49:01 до 02.10.2026 8:49:01 Пользователь: Колушкин С.А.	
Григорьев В.И. - Проректор по общим вопросам и цифровизации (Ректорат)	Согласен	23.10.2025 15:49	Электронная подпись Сертификат: 2E9F92A854A11A8F409AD76A553B1694 Кем выдан: uc_fk@roskazna.ru, 77 Москва, 7710568760, 1047797019830, Большой Златоустинский переулок, д. 6, строение 1, г. Москва, RU, Казначейство России, Федеральное казначейство Кому выдан: RU, Тульская область, проректор по общим вопросам и цифровизации, Ректорат, ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ТУЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ", 06871311471, 613502394519, oib@tsu.tula.ru, Владимир Иванович, Григорьев, Григорьев Владимир Иванович Действителен: с 28.07.2025 10:27:08 до 21.10.2026 10:27:08 Пользователь: Григорьев В.И.	
Меленкова Н.С. - Документовед общего отдела (Общий отдел)	Принят к утверждению общим отделом	24.10.2025 09:33		

Подготовил: Меленкова Н.С. (24.10.2025 9:33:40)

Подтверждаю

Приложение
к приказу от 24.10.2025 № 1803

План мероприятий по защите информации, обрабатываемой в информационных системах персональных данных

1. Общие положения

1.1. План мероприятий по защите информации в информационных системах персональных данных (далее – План) разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 152- ФЗ «О персональных данных», Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. План содержит необходимый перечень мероприятий для обеспечения безопасности информации и их периодичность.

1.3. Мероприятия по защите информации осуществляются Ответственным за организацию обработки ПДн, Администратором в рамках своих должностных обязанностей / должностных инструкций, Ответственным пользователем средств криптографической защиты в рамках выполнения своих обязанностей.

1.4. По результатам проведения мероприятия Администратор осуществляет соответствующую запись в Журнале учета мероприятий по контролю обеспечения защиты информации.

1.5. Контроль выполнения мероприятий по обеспечению защиты информации осуществляется Ответственным за организацию обработки ПДн и/или руководством Оператора.

2. План мероприятий

Мероприятие	Периодичность	Исполнитель/ Ответственный
Проверка наличия обновлений базы данных признаков вредоносных компьютерных программ и обновление при необходимости	Ежедневно / в случае возникновения инцидента	Администратор
Проверка рабочих станций и работоспособности средств защиты информации, в т.ч. СКЗИ	Ежеквартально / в случае возникновения инцидента	Администратор, Ответственный пользователь средств криптографической защиты
Проверка наличия документов, подтверждающих возможность применения средств защиты (сертификатов соответствия и других документов), обновление средств защиты информации при необходимости	Ежеквартально / в случае возникновения инцидента	Администратор, Ответственный пользователь средств криптографической защиты
Проверка журналов учета событий, регистрируемых средствами защиты	Еженедельно / в случае возникновения инцидента	Администратор
Проверка журнала учета событий, регистрируемых операционной системой	В случае возникновения инцидента	Администратор
Контроль смены паролей пользователей, проверка соблюдения требований парольной политики	1 раз в 180 дней / в случае возникновения инцидента	Администратор
Заведение, удаление учетных записей пользователей; наделение, лишение, изменение полномочий пользователей по доступу к ресурсам ИСПДн	По мере необходимости (в случае изменений в структуре ИСПДн и (или) обработке информации, штатных изменений)	Администратор
Выявление, анализ и устранение уязвимостей ПО и сканирование сетевых портов	Ежеквартально / в случае возникновения инцидента	Администратор
Проведение тестирования на проникновение, подтверждающего возможность использования выявленных уязвимостей или выявления новых сценариев реализации угрозы безопасности	Ежегодно	Администратор

Обновление контента безопасности средства анализа защищенности	Перед проведением сканирования	Администратор
Настройка и обновление программного обеспечения	При выпуске производителем критических обновлений и обновлений безопасности	Администратор
Резервное копирование данных[1]	Еженедельно	Администратор
Создание эталонных копий ПО	Ежемесячно / при внесении изменений в эталонные копии	Администратор
Проведение мероприятий по обучению пользователей ИСПДн по вопросам обеспечения защиты информации	1 раз в 2 года (внепланово может проводиться по мере внесений изменений в Законодательство РФ, внедрении новых СЗИ, выявления новых угроз безопасности информации и т.д.)	Администратор, Ответственный пользователь средств криптографической защиты, Ответственный за организацию обработки ПДн
Актуализация/ доработка организационно-распорядительных документов, регламентирующих обработку и защиту информации	В случае изменений в структуре, составе ИСПДн и (или) обработке информации, штатных изменений, а также по мере внесений изменений в Законодательство РФ	Администратор, Ответственный пользователь средств криптографической защиты
Ведение Журналов, необходимых для выполнения требований законодательства РФ в сфере обработки и защиты информации	По мере необходимости	Администратор, Ответственный пользователь средств криптографической защиты, Ответственный за организацию обработки ПДн
Пересмотр модели угроз безопасности информации	В случае: – изменения требований нормативных правовых актов, регламентирующих вопросы оценки угроз безопасности информации; – изменений архитектуры и условий функционирования ИСПДн, режима обработки ПДн, правового режима информации, влияющих на угрозы безопасности информации; – выявления новых угроз безопасности информации или новых сценариев реализации существующих угроз; включения в банк данных	Администратор

[1] Осуществляется в автоматическом режиме, администратор задает настройки резервирования

	угроз безопасности информации ФСТЭК России сведений о новых угрозах, сценариях (тактиках, техниках) их реализации	
Контроль за соблюдением режима обработки ПДн	Раз в полгода (внепланово может проводиться при поступлении информации о нарушениях правил обработки ПДн)	Ответственный за организацию обработки ПДн
Контроль за обеспечением уровня защиты информации	Не реже 1 раз в 2 года	Комиссия из состава работников Оператора / организация-лицензиат ФСТЭК России
Контроль выполнения мероприятий, предусмотренных Планом мероприятий по защите информации	Ежегодно	Ответственный за организацию обработки ПДн; Ответственный за обеспечение безопасности