МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
(УУНиТ)

ПРИКАЗ

22.08.2025 № 2348

Уфа

Об утверждении Плана мероприятий по выполнению рекомендаций по результатам оценки защищенности информационных ресурсов

В соответствии со статьей 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и подпунктом «в» пункта 5 Указа Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», п р и к а з ы в а ю:

1. Утвердить прилагаемый План мероприятий по выполнению рекомендаций, данных по итогам мероприятий по оценке защищенности информационных ресурсов Уфимского университета науки и технологий (далее – План).

2. Назначить начальника отдела защиты информации (далее – ОЗИ) Галиева С.Р. ответственным за:

2.1. координацию работ по выполнению утвержденного Плана;

2.2. контроль полноты, сроков и качества выполнения мероприятий, предусмотренных Планом;

2.3. своевременное внесение в План сведений о выполнении мероприятий;

2.4. взаимодействие с задействованными структурными подразделениями УУНиТ и его филиалами по вопросам реализации Плана;

2.5. подготовку и представление проректору по цифровой трансформации до 5-го числа месяца, следующего за отчетным, сводного отчета о ходе выполнения Плана.

3. Начальнику ОЗИ Галиеву С.Р.:

3.1. провести в срок до 10 сентября 2025 года организационное совещание с ответственными представителями структурных подразделений УУНиТ и филиалов по вопросам исполнения настоящего приказа и реализации Плана;

3.2. на период своего временного отсутствия (отпуск, командировка, болезнь) обеспечить делегирование полномочий по контролю за выполнением Плана сотруднику отдела с представлением соответствующего приказа на утверждение.

4. Директорам филиалов УУНиТ обеспечить до 20 октября 2025 года проведение во взаимодействии с ОЗИ внутреннего мониторинга защищенности информационных ресурсов филиалов, включающего:

4.1. сбор и анализ сведений о принадлежащих и используемых филиалом информационных ресурсах;

4.2. инвентаризацию функционирующих информационных сервисов и выявление уязвимостей;

4.3. оценку защищенности информационных ресурсов.

5. Директорам филиалов Университета обеспечить до 03 ноября 2025 года:

5.1. разработку проекта плана мероприятий по повышению защищенности информационных ресурсов филиала;

5.2. его согласование с отделом защиты информации и проректором по цифровой трансформации;

5.3. утверждение указанного плана соответствующим приказом и организацию его выполнения.

6. Общему отделу в срок не позднее 2 рабочих дней с даты издания настоящего приказа довести настоящий приказ до сведения руководителей структурных подразделений (работников), указанных в настоящем приказе и Плане.

7. Настоящий приказ вступает в силу со дня его подписания.

8. Контроль за исполнением настоящего приказа возложить на проректора по цифровой трансформации Хайбуллина А.Р.

Ректор В.П. Захаров

Приложение к приказу УУНиТ от 22.08.2025 № 2348

План мероприятий по выполнению рекомендаций, данных в рамках
мероприятий по оценке защищенности информационных ресурсов Уфимского университета науки и технологий

№ п/п	Рекомендации по устранению выявленных недостатков (нарушений)	Проведенные мероприятия	Срок исполнения	Ответственный исполнитель	Отметка об исполнении
1.	Скорректировать парольную политику и организовать смену паролей (в соответствии с рекомендациями, приведенными в политике по организации парольной защиты) скомпрометированных учетных записей, используемых для доступа к объектам ИТС.	Издание приказа УУНиТ по вопросам парольной политики. Рассылка служебной записки в структурные подразделения для смены паролей в соответствии с рекомендациями, приведенными в политике по организации парольной защиты	1 квартал 2026 г.	Отдел защиты информации	
2.	Провести инвентаризацию сетевых объектов ИТС на предмет использования учетных записей со словарными (нестойкими к атакам, направленных на их перебор) или установленными «по умолчанию» паролями, а также с паролями с неограниченным сроком действия	Приказ об инвентаризации сетевых объектов ИТС. Служебная записка в УЦИ от ОЗИ для смены паролей.	1 квартал 2026 г.	Отдел защиты информации, Управление цифровой инфраструктуры	

№ п/п	Рекомендации по устранению выявленных недостатков (нарушений)	Проведенные мероприятия	Срок исполнения	Ответственный исполнитель	Отметка об исполнении
3.	Исключить практику хранения пользователями и/или администраторами на своих рабочих станциях и общих сетевых ресурсах аутентификационных данных в открытом виде	Разработка правил по хранению аутентификационных данных. Рассылка служебной записки в структурные подразделения о недопущении хранения пользователями аутентификационных данных в открытом виде. Регулярный аудит хранения и использования паролей и учетных данных. Обнаружение и устранение случаев хранения в открытом виде	Постоянно	Отдел защиты информации, Управление цифровой инфраструктуры	
4.	Провести инвентаризацию объектов ИТС Учреждения на предмет наличия на них работающих САВЗ с актуальными БДКВ. В случае отсутствия САВЗ произвести их установку	Приказ о необходимости ответственных лиц в структурных подразделениях об установке САВЗ на АРМ. Ведение реестра установленных САВЗ и постоянный аудит на актуальность БДКВ.	1 квартал 2026 г.	Отдел защиты информации, Управление цифровой инфраструктуры, подразделения институтов и факультетов	
5.	Провести обновление используемого на объектах ИТС Учреждения ПО, содержащего критические уязвимости, с целью минимизации возможностей внутреннего и внешнего злоумышленников по воздействию на ресурсы и объекты ИТС Учреждения (обновления ПО могут быть получены на сайтах его разработчиков). В случае отсутствия такой возможности провести корректировку настроек ПО и используемых СЗИ с целью минимизации возможности эксплуатации уязвимостей	Аудит ПО, содержащего критические уязвимости. Ведение реестра.	Постоянно	Отдел защиты информации, Управление цифровой инфраструктуры	
6.	Провести мероприятия, направленные на реализацию положений Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ	Утвержден перечень объектов КИИ, подлежащих категорированию	В течение 2026 г.	Отдел защиты информации	

№ п/п	Рекомендации по устранению выявленных недостатков (нарушений)	Проведенные мероприятия	Срок исполнения	Ответственный исполнитель	Отметка об исполнении
7.	Разработать документы по информационной безопасности, в которых будут отражены:	Разработка документов. Приказ об утверждении.	В течение 2026 г.	Отдел защиты информации, Управление цифровой инфраструктуры	
7.1.	политика маршрутизации сетевого трафика внутри ИТС, в которой предусмотреть ограничение сетевого взаимодействия между сегментами ИТС, ограничение сетевого доступа к управляющим интерфейсам ТКО, серверам, рабочим станциям администраторов, системам резервного копирования информации, ключевому оборудованию ИТС				
7.2.	порядок использования внешних USB-устройств на рабочих станциях пользователей ИТС				
7.3.	порядок предоставления административных привилегий пользователям ИТС				
7.4.	порядок получения дополнительных привилегий пользователями ИТС				
7.5.	порядок обновления ПО				
7.6.	регламент использования и защиты БСПД на объектах Учреждения, а также их взаимодействия с другими объектами ИТС				
8.	Рассмотреть возможность замены используемого на объектах ИТС Учреждения общесистемного ПО, официальная поддержка которого прекращена производителем. В случае отсутствия такой возможности проводить периодическую корректировку настроек ПО и используемых СЗИ с целью минимизации возможности эксплуатации уязвимостей	Аудит. При необходимости разработка регламента с последующим его утверждением приказом УУНиТ.	31.12.2025	Проректор по цифровой трансформации, Отдел защиты информации, Управление цифровой инфраструктуры	
9.	Произвести настройку САВЗ «Kaspersky Security Center» в соответствии с «Руководством по усилению защиты», размещенным на портале «support.kaspersky.ru»	Настройка САВЗ «Kaspersky Security Center» в соответствии с «Руководством по усилению защиты»	31.01.2026	Отдел защиты информации	

№ п/п	Рекомендации по устранению выявленных недостатков (нарушений)	Проведенные мероприятия	Срок исполнения	Ответственный исполнитель	Отметка об исполнении
10.	Провести инвентаризацию сетевых ресурсов ИТС Учреждения на предмет выявления целесообразности предоставления к ним анонимного доступа. Исключить возможность анонимного доступа к сетевым ресурсам, содержащим критические для Учреждения данные	Приказ о инвентаризации сетевых ресурсов ИТС. Настройка доступа к сетевым ресурсам, содержащим критические данные.	31.12.2025	Отдел защиты информации, Управление цифровой инфраструктуры	
11.	Организовать во всех подразделениях Учреждения функционирование рабочих станций пользователей ИТС с применением доменной архитектуры	Закупка отечественного ПО и оборудования. Настройка доменной архитектуры.	по мере выделения финансирования в установленном порядке	Управление цифровой инфраструктуры	
12.	Произвести инвентаризацию объектов ИТС на предмет необходимости наличия у пользователей административных привилегий. Предоставлять пользователям ИТС Учреждения указанные привилегии только на основании обоснованных заявок на минимально необходимый промежуток времени	Приказ о инвентаризации объектов ИТС на предмет необходимости наличия у пользователей административных привилегий. Предоставление пользователям ИТС Учреждения административных привилегии только на основании обоснованных заявок.	1-2 квартал 2026 г.	Отдел защиты информации, Управление цифровой инфраструктуры	
13.	Средствами ТКО произвести ограничение взаимодействия между различными сегментами ИТС Учреждения в соответствии с разработанной политикой маршрутизации сетевого трафика	Настройка в соответствии с политикой маршрутизации сетевого трафика.	В течение 2026 г.	Отдел защиты информации, Управление цифровой инфраструктуры	
14.	Исключить возможность доступа пользователей ИТС к нежелательным ресурсам сети Интернет (в том числе к сторонним сервисам VPN, анонимизации)	Настройка контент-фильтра.	Постоянно	Отдел защиты информации, Управление цифровой инфраструктуры	
15.	Исключить взаимодействие объектов ИТС Учреждения с сетью Интернет без применения МСЭ	Настройка МСЭ для исключения взаимодействия объектов ИТС Учреждения с сетью Интернет.	В течение 2026 г.	Отдел защиты информации, Управление цифровой инфраструктуры	

№ п/п	Рекомендации по устранению выявленных недостатков (нарушений)	Проведенные мероприятия	Срок исполнения	Ответственный исполнитель	Отметка об исполнении
16.	Организовать контроль подключений к ИТС Учреждения сетевых объектов, не входящих в ее состав	Приказ о контроле подключений к ИТС Учреждения сетевых объектов, не входящих в ее состав.	Постоянно	Отдел защиты информации	
17.	Рассмотреть возможность отключения протоколов NBNS и LLMNR. В случае необходимости использования указанных протоколов, установить статические записи для основных узлов сети (шлюз по умолчанию, серверы), а также использовать WINS-сервер вместо широковещательных запросов	Аудит. При необходимости разработка регламента.	31.11.2025	Отдел защиты информации, Управление цифровой инфраструктуры	
18.	Провести инвентаризацию объектов ИТС на предмет включенной поддержки неиспользуемого протокола IPv6 с небезопасными настройками «по умолчанию». В случае обнаружения на оконечных устройствах, отключить неиспользуемый протокол Ipv6. Установить фильтрацию Ipv6 пакетов на маршрутизаторах. В случае невозможности отключения скорректировать настройки безопасности сетевого взаимодействия, связанные с использованием указанного протокола	Приказ об инвентаризации объектов ИТС на предмет включенной поддержки неиспользуемого протокола IPv6. Настройка и корректировка.	В течение 2026 г.	Отдел защиты информации, Управление цифровой инфраструктуры	
19.	Исключить использование на объектах ЛВС службы автоматической настройки прокси WPAD	Приказ об исключении использования автоматической настройки прокси WPAD на объектах ЛВС.	31.12.2025	Отдел защиты информации, Управление цифровой инфраструктуры	
20.	Организовать применение в ИТС механизмов защиты от атак, направленных на перехват сетевого трафика. В частности, рассмотреть возможность использования на сетевом оборудовании следующих механизмов защиты: DHCP v4 snooping, NDP snooping, DHCP v4 Guard, DHCP v4-Shield, IP Source Guard, Dynamic ARP inspection, Rogue Device detection	Настройка и корректировка механизмов защиты от атак, направленных на перехват сетевого трафика.	В течение 2026 и 2027 гг.	Отдел защиты информации, Управление цифровой инфраструктуры	

№ п/п	Рекомендации по устранению выявленных недостатков (нарушений)	Проведенные мероприятия	Срок исполнения	Ответственный исполнитель	Отметка об исполнении
21.	Отказаться от использования для удаленного администрирования объектов ИТС Учреждения незащищённых протоколы HTTP, Telnet, в случае невозможности, произвести сетевое изолирование управляющих интерфейсов	Приказ об инвентаризации систем и ресурсов для удаленного администрирования объектов ИТС.	31.12.2025	Отдел защиты информации, Управление цифровой инфраструктуры	
22.	Включить требование использования цифровой подписи SMB и LDAP сообщений для всех объектов ИТС	Приказ о требовании использования цифровой подписи SMB и LDAP.	1-2 квартал 2026 г.	Отдел защиты информации, Управление цифровой инфраструктуры	
23.	Исключить возможность использования на объектах ИТС Учреждения ПО для удаленного доступа, использующего сторонние серверы	Приказ о запрете использования ПО для удаленного доступа, использующего сторонние серверы.	1-3 квартал 2026 г.	Отдел защиты информации, Управление цифровой инфраструктуры	
24.	Организовать контроль подключений съемных носителей информации и внешних USB-устройств к объектам ИТС Учреждения	Контроль и ведение реестра подключений съемных носителей информации и внешних USB-устройств к объектам ИТС Учреждения.	Постоянно	Отдел защиты информации	
25.	Отключить на рабочих станциях пользователей ИТС Учреждения возможность изменения настроек BIOS/UEFI, а также загрузку рабочих станций с внешних носителей информации	Распоряжение об отключении изменение настроек BIOS/UEFI.	В течение 2026 и 2027 гг.	Отдел защиты информации, Управление цифровой инфраструктуры	
26.	Добавить все критически важные учетные записи домена «ugatu-ad.local» в группу «Protected Users»	Настройка и корректировка домена.	В течение 2026	Управление цифровой инфраструктуры	
27.	Исключить возможность создания машинных учетных записей в домене «ugatu-ad.local» непривилегированными пользователями	Настройка и корректировка домена.	В течение 2026	Управление цифровой инфраструктуры	
28.	Организовать Контроль действий подрядных организаций, обслуживающих различные ИС Учреждения. Предоставлять доступ только к необходимым ИС Учреждения на минимально необходимый промежуток времени	Контроль и ведение реестра подключений подрядных организаций.	Постоянно	Отдел защиты информации, Управление цифровой инфраструктуры	

№ п/п	Рекомендации по устранению выявленных недостатков (нарушений)	Проведенные мероприятия	Срок исполнения	Ответственный исполнитель	Отметка об исполнении
29.	Рассмотреть вопрос целесообразности использования в ИТС БСПД. В случае наличия такой необходимости разработать регламент использования БСПД на территории Учреждения и ее взаимодействия с другими объектами ИТС, организовать подключение оборудования, предназначенного для организации БСПД, к ИТС с использованием средств межсетевого экранирования	Аудит БСПД. При необходимости разработка регламента.	31.12.2025	Отдел защиты информации, Управление цифровой инфраструктуры	
30.	Организовать настройку и функционирование системы мониторинга состояния и доступности критически важных объектов ИТС Учреждения	Приказ о введении в эксплуатацию системы мониторинга.	В течение 2026 и 2027 гг.	Отдел защиты информации, Управление цифровой инфраструктуры	

ПРОЕКТ ВНОСИТ

Проректор по цифровой трансформации	**5922421**	А. Р. Хайбуллин
Должность	29.08.2025 09:30:08 подпись	расшифровка подписи

СОГЛАСОВАНО

ОМиСУП Заместитель начальника Должность	**5922456** 29.08.2025 09:32:06 подпись	Барышева А. И. расшифровка подписи	комментарий
ОЗИ Начальник Должность	**5886310** 25.08.2025 09:27:17 подпись	Галиев С. Р. расшифровка подписи	комментарий
Проректор по общим вопросам Должность	**5888113** 25.08.2025 11:14:41 подпись	Магзумов Р. Р. расшифровка подписи	комментарий
ОЗГТ Начальник Должность	**5887074** 25.08.2025 10:13:37 подпись	Бикмулина М. Е. расшифровка подписи	комментарий
Бирский филиал УУНиТ Директор Должность	**5887414** 25.08.2025 10:34:21 подпись	Ганеев В. В. расшифровка подписи	комментарий
СФ УУНиТ Должность	**5892279** 25.08.2025 17:14:46 подпись	Сыров И. А. расшифровка подписи	комментарий
НФ УУНиТ Директор, к.н., доцент Должность	**5886684** 25.08.2025 09:49:53 подпись	Шаяхметов Н. Н. расшифровка подписи	комментарий
СИ УУНиТ Директор Должность	**5887932** 25.08.2025 11:05:44 подпись	Хамитов И. С. расшифровка подписи	комментарий
Филиал УУНиТ в г. Кумертау Директор Должность	**5886607** 25.08.2025 09:44:02 подпись	Фахруллина А. Р. расшифровка подписи	комментарий
Филиал ФГБОУ ВО «УУНиТ» в г. Ишимбае Должность	**5893200** 25.08.2025 19:03:21 подпись	Хуснутдинов Д. З. расшифровка подписи	комментарий
УЦИ Начальник Должность	**5897458** 26.08.2025 12:41:37 подпись	Ямилов И. Р. расшифровка подписи	комментарий
ФЭУ	**5888371**	Валиуллина О. Д.	

Заместитель начальника Должность	25.08.2025 11:29:56 подпись	расшифровка подписи	комментарий
ПУ Начальник Должность	**5921478** 28.08.2025 19:20:57 подпись	Манукян Н. Г. расшифровка подписи	комментарий
ЦБ Главный бухгалтер Должность	**5886542** 25.08.2025 09:39:59 подпись	Колохова Г. Р. расшифровка подписи	комментарий
ФЭУ Заместитель начальника Должность	**5888387** 25.08.2025 11:30:15 подпись	Валиуллина О. Д. расшифровка подписи	комментарий

ИСПОЛНИТЕЛЬ

Проректор по цифровой трансформации Должность	подпись	Хайбуллин А. Р. расшифровка подписи

162870