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

ПРИКАЗ

21.12.2023 № 3325

Уфа

Об утверждении Политик по организации антивирусной и парольной защит ФГБОУ ВО «Уфимский университет науки и технологий»

В целях обеспечения информационной безопасности в ФГБОУ ВО «Уфимский университет науки и технологий» в соответствии с Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», п р и к а з ы в а ю:

1. Утвердить:

1.1. «Политику по организации антивирусной защиты ФГБОУ ВО «Уфимский университет науки и технологий» (Приложение № 1).

1.2. «Политику по организации парольной защиты ФГБОУ ВО «Уфимский университет науки и технологий» (Приложение № 2).

2. Общему отделу обеспечить рассылку настоящего приказа проректорам, во все структурные подразделения.

3. Руководителям структурных подразделений:

3.1. Ознакомить сотрудников с Политиками под личную роспись.

3.2. Осуществлять внутренний контроль над исполнением требований Политик в подразделении.

3. Настоящий приказ вступает в силу с момента подписания.

4. Контроль за исполнением настоящего приказа возложить на проректора по цифровой трансформации А.С. Борисова.

Ректор В.П. Захаров

Приложение № 1
к приказу от 21.12.2023 № 3325
«Об утверждении Политик по организации антивирусной и парольной защит федеральном государственном бюджетном образовательном учреждении высшего образования «Уфимский университет науки и технологий»

Политика
по организации антивирусной защиты
ФГБОУ ВО «Уфимский университет науки и технологий»

Уфа
2023

Содержание

1 Общие положения

1.1 Настоящая политика определяет требования к организации защиты информационных ресурсов ФГБОУ ВО «Уфимский университет науки и технологий» (далее – Университет) от воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее - вредоносного ПО), устанавливает ответственность руководителей и сотрудников, эксплуатирующих и сопровождающих информационные ресурсы Университета.

1.2 Настоящая политика определяет порядок применения средств антивирусной защиты в Университете и структурных подразделениях, задачи, обязанности, права и ответственность сотрудников отдела защиты информации (далее – отдел ЗИ) и пользователей автоматизированных рабочих мест (далее – АРМ), порядок установки, обновления и применения средств антивирусной защиты (далее – САВЗ), также порядок ликвидации последствий воздействия вирусов.

1.3 Требования настоящей политики обязательны для выполнения всеми сотрудниками Университета.

1.4 Целью организации антивирусной защиты является:

- предотвращение потерь информации;
- защита информационных ресурсов Университета от несанкционированного копирования, искажения и разрушения;
- минимизация риска сбоев и отказов в работе информационных процессов при воздействии вирусов;
- минимизация финансовых потерь и трудовых затрат при устранении последствий воздействий вирусов.

1.5 Задачами антивирусной защиты являются:

- проведение профилактических работ с применением антивирусных диагностических средств;
- непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации ин6формационных ресурсов Университета.

1.6 Компоненты информационных ресурсов Университета, подлежащее защите от вирусов:

- интернет шлюзы, установленные в точках подключения к сетям общего пользования, а также ведомственным сетям;
- сервера;
- АРМ

1.7 Основные источники вирусов:

- съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;
- локальная сеть, в том числе система электронной почты и Интернет;
- жесткий диск, на который попал вирус в результате работы с зараженными программами.

1.8 Основные признаки появления вирусов:

- прекращение работы или неправильная ранее успешно функционировавших программ;
- медленная работа АРМ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размера файлов;

- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе АРМ.

2. Организация мероприятий по антивирусной защите

2.1 Ответственность за контроль организации антивирусной защиты информации, управлением антивирусной защитой и контроль выполнения настоящей политики возлагается на отдел ЗИ.

2.2 На всех АРМ сотрудников должны быть установлены лицензионные и сертифицированные ФСТЭК России средства антивирусной защиты. Удаление, отключение, несанкционированное изменение настроек, конфигураций средства антивирусной защиты запрещается.

2.3 Работа без установленного средства антивирусной защиты информации на АРМ не допускается.

2.4 Обновление антивирусных баз должно производиться в автоматическом режиме. В случае сбоя автоматического обновления обновление баз должно производится вручную.

2.5 Мероприятия по антивирусной защите включают в себя:
- профилактика вирусов;
- анализ ситуаций;
- применение средств антивирусной защиты;
- проведение расследований инцидентов, связанных с вирусами.

3. Профилактика вирусов

3.1 Регулярно проводимые профилактические работы по выявлению вирусов могут полностью исключить появление и распространение вирусов. К основным профилактическим работам и мероприятиям относятся:
- ежедневная автоматическая быстрая антивирусная проверка;
- ежеквартальная выборочная проверка серверов БД на наличие вирусов бесплатными антивирусными утилитами, даже при отсутствии внешних проявлений вирусов;
- изучение информации по сообщениям в журналах и Интернете о новых вирусах и их способах распространения и заражения и информирование сотрудников Университета о новых способах распространения вредоносного ПО и других актуальных угрозах;
- ограничение доступа к компонентам ИС Университета третьих лиц.

3.2 При обнаружении вирусов на АРМ и серверах, работающих в локальной сети, внеплановой проверке подлежат все АРМ и сервера, входящие в один сегмент сети с зараженным АРМ или сервером, или работающие с общими данными и программным обеспечением.

4. Анализ ситуаций

4.1 При возникновении подозрения на наличие вредоносного ПО (ошибки в работе программ, появление графических и звуковых эффектов, искажения данных, пропадание файлов, частое появление сообщений о системных ошибках, замедление работы компьютера и т.п.) сотрудник самостоятельно может провести внеочередной антивирусный контроль, либо обратиться в отдел ЗИ.

4.2 При возникновении подозрения на наличие вредоносного ПО на серверах и интернет-шлюзах сотрудники отдела ЗИ организует осуществление внеочередного антивирусного контроля.

4.3 При обнаружении вредоносного ПО сотрудники отдела ЗИ выполняет анализ ситуации. В результате анализа делается вывод о способе уничтожении вирусов.

5. Применение средств антивирусной защиты

5.1 Лечение или уничтожение вредоносного ПО осуществляется в автоматическом режиме средствами антивирусной защиты, а в ситуациях, когда это невозможно – вручную.

5.2 В случае уничтожения вредоносным ПО файлов баз данных и содержащихся на файловом сервере данных, сотрудники отдела ЗИ организуют их восстановление, используя последнюю резервную копию.

5.3 После уничтожения вредоносного ПО и восстановления зараженных файлов необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы. Перед повторной проверкой необходимо перезагрузить компьютер.

5.4 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях.

5.5 Файлы, помещаемые на архивное хранение, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в квартал в ручном или автоматическом режиме.

5.6 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на предмет отсутствия вредоносных файлов.

6. Ответственность

6.1 За невыполнение требований настоящего Положения может быть применена дисциплинарная ответственность в порядке, определенным законодательством Российской Федерации и локальными актами Университета.

ЛИСТ ОЗНАКОМЛЕНИЯ

С Политикой по организации антивирусной защиты ФГБОУ ВО «Уфимский университет науки и технологий»

(наименование)

С политикой по организации антивирусной защиты ознакомлен и обязуюсь выполнять:

п/п	Ф.И.О.	Должность	Дата	Подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

Приложение № 2
к приказу от 21.12.2023 № 3325
«Об утверждении Политик по организации антивирусной и парольной защит федеральном государственном бюджетном образовательном учреждении высшего образования «Уфимский университет науки и технологий»

Политика
по организации парольной защиты
ФГБОУ ВО «Уфимский университет науки и технологий»

Уфа
2023

Содержание

1. Общее положение

1.1. Политика устанавливает основные правила введения парольной защиты в ФГБОУ ВО «Уфимский университет науки и технологии» (далее – Университет), является внутренним документом и подразумевает запрет передачи данного документа за пределы Университета.

1.2. Настоящая политика регламентирует организационно-техническое обеспечение процессов генерации и смены паролей от всех эксплуатируемых вычислительных ресурсов и информационных систем, меры обеспечения безопасности при использовании паролей, а также контроль за действиями сотрудников университета при работе с паролями.

1.3. Положения и требования данного документа распространяются на все структурные подразделения университета, включая филиалы и являются обязательными для выполнения всеми работниками университета.

1.4. Законодательной основой настоящей Политики являются:

- Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных»;
- Инструкция о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки Российской Федерации, утвержденная Приказом Министерства образования и науки Российской Федерации от 30.12.2010 №2233;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Цель (назначение) Политики

2.1. Политика направлена на защиту доступа к эксплуатируемым вычислительным ресурсам и информационным системам в целях недопущения утечки данных, а также их несанкционированной модификации или уничтожения.

2.2. Политика определяет требования Университета к парольной защите информационных систем, организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах организации и контроль за действиями исполнителей.

2.2. Политика направлена на минимизацию риска несанкционированного доступа к информационным системам Университета, за счет использования слабостей в организации парольной защиты

2.3. Техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей.

2.4. Ознакомление всех работников университета, использующих средства вычислительной техники.

3. Объекты защиты

3.1. Объектами, подлежащими защите в соответствии с Настоящей политикой, являются:

- информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации,

системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной среды.

4. Порядок создания паролей

4.1. Пароли доступа создаются на всех компонентах автоматизированного рабочего места (далее – АРМ) и информационных систем Университета (далее ИС Университета), имеющих механизмы идентификации и аутентификации.

4.2. Создание паролей доступа осуществляется лицами, осуществляющие администрирование АРМ и ИС Университета соответственно.

Для «Информационной системы управления университетом» УУНиТ пароль создается самим Пользователем при создании учетной записи.

4.3. При заведении нового Пользователя для него должен быть назначен логин и однократный пароль.

4.4. Пользователь обязан заменить однократный пароль – личным при первом же подключении к защищаемому ресурсу АРМ и ИС Университета.

4.5. При отсутствии возможности создания однократного пароля, с последующей сменой Пользователем, создается постоянный пароль.

4.6. Одноразовый пароль может передаваться Пользователю лично на бумажном носителе, в электронном виде на адрес индивидуальной рабочей электронной почты или в устной форме.

4.7. Постоянный пароль передается Пользователю в запечатанном конверте.

4.8. Пользователь обязан хранить в тайне пароль и любые другие средства доступа к информационным ресурсам.

4.9. Пароли от учетных записей, обладающих правами администратора, могут выдаваться только лицам, осуществляющим администрирование АРМ и ИС Университета.

5. Период действия и порядок смены паролей

5.1. Периодичность смены паролей для АРМ и ИС Университета должна проводиться регулярно, не реже одно раза в три месяца.

5.2. При сообщении об окончании срока действия пароля АРМ и ИС Университета Пользователь обязан заменить его на новый, ранее не применявшийся.

5.3. Смена паролей в АРМ и ИС Университета, не имеющем функционал установления срока действия пароля, осуществляется лицами, осуществляющим администрирование АРМ и ИС Университета в соответствии с установленной периодичностью.

5.4. Внеплановая смена пароля или блокирование учетных записей Пользователя в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться в течение двух рабочих часов после получения копии приказа о прекращении полномочий.

5.5. Внеплановая смена паролей учетных записей, обладающих правами Администратора, должна производиться в случае прекращения полномочий (увольнение, переход на другую работу, окончание действия договора на обслуживание и другие обстоятельства) лицами, осуществляющим администрирование АРМ и ИС Университета

5.6. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов средств защиты

или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.

5.7. Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИС Университета.

5.8. В случае компрометации личного пароля пользователя надлежит незамедлительно уведомить Отдел защиты информации до момента вступления в силу новой учетной записи пользователя или пароля.

6. Конфиденциальность паролей

6.1. Информация о персональных паролях Пользователей является конфиденциальной информацией и разглашению не подлежит.

6.2. Пользователи несут ответственность за сохранность выбранного самостоятельно постоянного пароля и за действия, совершаемые под выданной Пользователю учетной записью.

6.3. Компоненты ИС Университета должны быть настроены таким образом, чтобы исключить возможность ознакомления Пользователей и лиц, обладающих правами администратора, с действующими и истекшими паролями.

7. Правила генерации паролей

7.1. Личные пароли пользователей АРМ и ИС Университета должны выбираться в соответствии с настоящей политикой с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать латинские буквы, цифры и (или) специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd, и т.п.).

7.2. При смене пароля запрещается использовать ранее использованные пароли, а новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

7.3. Выбор паролей служебных и привилегированных учетных записей АРМ и ИС Университета осуществляется по тем же требованиям, за исключением длины пароля – она должна быть не менее 12 символов.

- в числе символов пароля обязательно должны присутствовать, латинские буквы, цифры и (или) специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd, и т.п.), пароль не должен быть словом русского либо английского языка, в котором заменены некоторые символы (o->0,s->$, a->@ и т.п.).
- при смене пароля новый пароль должен отличаться от старого не менее, чем четырьмя символами, расположенными не подряд.

8. Организация парольной защиты

8.1. Организация парольной защиты «Литера Н» УУНиТ:

- Пароли доступа пользователей к АРМ и ИС Университета первоначально формируются администратором локально вычислительной сети (далее ЛВС), а в дальнейшем выбираются пользователями самостоятельно, но с учетом требований правила генерации паролей п.7 настоящей Политики.

8.2. Организация парольной защиты «Литера Т»:

В Литере «Т» вход в систему осуществляется посредством учетных записей домена ugatu-ad.local. Замена пароля для пользователей домена осуществляется настройкой Администратора AD путем выбора всех имеющихся пользователей домена и последующей личной заменой каждым пользователей домена «Сменить пароль при входе». Информация о смененном пароле отправляется автоматически Администратору AD.

8.3. Замена пароля в Информационной системе управления университетом (далее – ИСУУ) УУНиТ осуществляется путем нажатия кнопки «Восстановить пароль». Далее будет необходимо ввести почту @ugatu.su или @uust.ru куда будет отправлено письмо для смены пароля.

8.4. В случае увольнения либо перехода в другое структурное подразделение, либо в случае длительного отпуска сотрудника отделом кадровой службы организации доводится информация до соответствующего отдела IT-инфраструктуры в целях блокировки учетной записи пользователя.

8.5. В случае увольнения системного администратора или сотрудника отдела IT-инфраструктуры отдел IT-инфраструктуры организации должен заблокировать доступ к эксплуатируемым вычислительным ресурсам и информационным системам, сменить все административные пароли.

8.6. Ознакомление всех сотрудников, использующих имеющих доступ к АРМ и ИС Университета, с требованиями настоящей политики проводят руководители структурных подразделений Университета (далее – отдел ЗИ).

9. Правила использования и сохранения в тайне личного пароля

9.1. Пароли необходимо запомнить. Допускается хранение паролей в индивидуальных сейфах и опечатываемых шкафах.

9.2. Пользователю запрещается:

- разглашать кому-либо персональный пароль и прочие идентифицирующее сведения;
- предоставлять доступ от своей учетной записи к информации, хранящиеся в ИС Университета посторонним лицам;
- предоставлять доступ к своей учетной записи другим Пользователям;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах, к которым могут иметь свободный доступ иные лица;
- сообщать посторонним лицам пароль для доступа к эксплуатируемым вычислительным ресурсам и информационным системам;
- оставлять рабочее место с инициализированным доступом к эксплуатируемым вычислительным ресурсам и информационным системам;
- осуществлять ввод пароля для доступа в систему в присутствии посторонних лиц;
- записывать пароли в общедоступных местах (монитор, обратная сторона клавиатуры, отдельные листы бумаги и т.д.);
- использовать повторно ранее использованные пароли;
- в настройках учетной записи создавать подсказки для паролей;
- создавать одинаковые (или идентичные) пароли для учетных записей, используемых в разных информационных системах.

9.3. В случае подозрения на компрометацию пароля, сотрудники обязаны:

- произвести экстренную замену личного пароля, при наличии такого права;
- незамедлительно поставить об этом в известность сотрудников отдела ЗИ для исключения возможности утечки информации;
- немедленно оповестить всех участников обмена информацией.

Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

9.4. Отдел ЗИ обязан произвести расследование причин компрометации пароля.

9.5. Под компрометацией следует понимать:

- передача идентификационной информации по открытым каналам связи;
- проникновение постороннего лица в помещение с АРМ или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
- проникновение вредоносного программного обеспечения или подозрение на него;
- перехват пароля при распределении идентификационной информации;
- сознательная передача идентификационной информации постороннему лицу.

9.6. Типовые случаи компрометации пароля:

- файлы, хранящиеся в ИС Университета, были несанкционированно изменены;
- изменено расположение иконок программ и файлов на рабочем столе АРМ и личных папках;
- при правильном вводе пароля выдается ошибка доступа;
- другие сотрудники знают ваш пароль.

10 Ответственность пользователей при работе с парольной защитой

10.1. Повседневный контроль за действиями сотрудников университета при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на отдел ЗИ Университета.

10.2. Владельцы паролей должны быть ознакомлены под подпись с перечисленными выше требованиями и предупреждены об ответственности за невыполнение требований.

10.3. Вход и использование ИС вне рабочего места и времени является личной ответственностью Пользователя.

10.4 За невыполнение требований настоящей Политики может быть применена дисциплинарная ответственность в порядке, определенным трудовым кодексом Российской Федерации и локальными актами Университета.

ЛИСТ ОЗНАКОМЛЕНИЯ

С Политикой по организации парольной защиты ФГБОУ ВО «Уфимский университет науки и технологий»

(наименование)

С политикой по организации парольной защиты ознакомлен и обязуюсь выполнять:

№ п/п	Ф.И.О.	Должность	Дата	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				

ПРОЕКТ ВНОСИТ

ОЗИ Начальник Должность	**1986567** 19.12.2023 13:45:06 подпись	А. Э. Габитов расшифровка подписи

СОГЛАСОВАНО

Проректор по цифровой трансформации Должность	**1968944** 15.12.2023 08:41:42 подпись	Борисов А. С. расшифровка подписи
Проректор по образовательной деятельности Должность	**1968224** 14.12.2023 18:52:31 подпись	Галимханов А. Б. расшифровка подписи
Проректор по развитию образования Должность	**1973475** 15.12.2023 15:41:49 подпись	Рахманова Ю. В. расшифровка подписи
Проректор по инновационной деятельности Должность	**1977140** 18.12.2023 09:45:59 подпись	Агеев Г. К. расшифровка подписи
УМС Начальник управления международного сотрудничества Должность	**1972993** 15.12.2023 15:12:43 подпись	Филипова Р. Ф. расшифровка подписи
Проректор по молодежной политике и воспитательной работе Должность	**1973948** 15.12.2023 16:20:09 подпись	Солодовник В. Н. расшифровка подписи
Проректор по стратегическому развитию Должность	**1968001** 14.12.2023 18:20:38 подпись	Янгиров А. В. расшифровка подписи
Проректор по организационному развитию Должность	**1967990** 14.12.2023 18:19:35 подпись	Кызыргулов И. Р. расшифровка подписи
Проректор по общим вопросам Должность	**1968111** 14.12.2023 18:37:12 подпись	Лебединцев П. В. расшифровка подписи
Проректор по содержанию и развитию имущественного комплекса Должность	**1968851** 15.12.2023 08:13:12 подпись	Магзумов Р. Р. расшифровка подписи

Профессор, д/н Должность	**1972637** 15.12.2023 14:40:29 подпись	Ямалова Э. Н. расшифровка подписи
Проректор по развитию филиальной сети Должность	**1982553** 18.12.2023 18:07:00 подпись	Мустафина С. А. расшифровка подписи
УП Начальник Должность	**1967912** 14.12.2023 18:07:46 подпись	Койда Л. А. расшифровка подписи
ФЭУ Начальник Должность	**1968471** 14.12.2023 21:01:39 подпись	Зюбан Э. В. расшифровка подписи
Главный бухгалтер Должность	**1967695** 14.12.2023 17:42:24 подпись	Колохова Г. Р. расшифровка подписи
ПУ Начальник Должность	**1989311** 19.12.2023 17:36:05 подпись	Манукян Н. Г. расшифровка подписи

ИСПОЛНИТЕЛЬ

ОЗИ Должность	подпись	Габитов А. Э. расшифровка подписи

70935