МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Астраханский государственный университет имени В.Н. Татищева» (Астраханский государственный университет им. В.Н. Татищева)

ПРИКАЗ

16.05.2024 № 08-01-01/899

Об утверждении Положения по соблюдению требований информационной безопасности в ФГБОУ ВО «Астраханский государственный университет им. В.Н. Татищева

В целях организации информационной безопасности в Университете

ПРИКАЗЫВАЮ:

1. Утвердить Положение по соблюдению требований информационной безопасности в ФГБОУ ВО «Астраханский государственный университет им. В.Н. Татищева».

2. Начальнику общего отдела Безниско М.И. довести настоящий приказ до руководителей и сотрудников структурных подразделений ФГБОУ ВО «Астраханский государственный университет им. В.Н. Татищева».

3. Контроль за исполнением настоящего приказа возложить на начальника службы охраны труда и безопасности Иванова М.Н.

И.о. ректора И.А. Алексеев

СОГЛАСОВАНО:

Проректор по общим вопросам Т.А. Манина

И.о. начальника отдела
нормативно-правового
обеспечения и противодействия коррупции Н.С. Гаврилова

Начальник общего отдела М.И. Безниско
15.05.2024

Начальник службы охраны труда
и безопасности М.Н. Иванов

И.о. начальника отдела
Информационной безопасности Д.Э. Шукралиева

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В.Н. Татищева»
(Астраханский государственный университет им. В.Н. Татищева)

СОГЛАСОВАНО:
Начальник службы охраны труда
и безопасности
_____ М.Н. Иванов
«16» 05 2024 г.

УТВЕРЖДЕНО:
Исполняющий обязанности ректора
_____ И.А. Алексеев
«16» 05 2024 г.

ПОЛОЖЕНИЕ
по соблюдению требований информационной безопасности в ФГБОУ ВО «Астраханский государственный университет им. В. Н. Татищева»

1. Общие положения

1.1. Настоящее Положение по соблюдению требований информационной безопасности в ФГБОУ ВО «Астраханский государственный университет им. В. Н. Татищева» по реализации защиты информационных ресурсов в «Астраханском государственном университете им. В. Н. Татищева» (далее – Университет) определяет требования к организации защиты информационных ресурсов Университета от воздействия вредоносного программного обеспечения и устанавливает ответственность руководителей и сотрудников подразделений, а также обучающихся Университета за их выполнение.

1.2. Положение разработано в целях установления общих правил, требований и процедур при взаимодействии подразделений Университета при реализации защиты информационных ресурсов.

1.3. Положение разработано с учетом следующих документов:

– Федерального закона от 08.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– приказа Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их

функционирования»;

– приказа Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Национального стандарта Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

– ФСТЭК России от 25.12.2017 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Методического документа Федеральной службы по техническому и экспортному контролю от 05.02.2021 «Методика оценки угроз безопасности информации».

1.4. Положение предназначено для сотрудников и обучающихся Университета, использующих средства вычислительной техники.

1.5. Положение устанавливает основные этапы деятельности при работе на автоматизированных рабочих местах с информационными ресурсами Университета.

2. Правила работы пользователей на автоматизированных рабочих местах

2.1 Средства вычислительной техники и автоматизированных систем Университета предоставляются пользователям исключительно для выполнения служебных обязанностей.

2.2 Пользователь автоматизированного рабочего места (далее – АРМ) обязан:

– проверять перед началом работы и уходом с работы целостности вверенного ему оборудования;

– блокировать рабочий стол АРМ при каждом покидании своего рабочего места;

– в случае обнаружения повреждений опломбирования или опечатывания системного блока, в случае если такое опечатывание проводилось – незамедлительно сообщить об этом в службу охраны труда и безопасности.

2.3 Пользователю АРМ запрещается:

– подключать личные средства вычислительной техники к корпоративной информационной сети (далее – КИС) Университет;

– использовать программные обеспечения (далее - ПО), не указанные в приложении 4 Политики информационной безопасности ФГБОУ ВО «Астраханский государственный университет им. В.Н. Татищева», утверждённой приказом от 13.02.2024 №08-01-01/251 (далее – Политика ИБ).

2.4 Для пользователей в качестве механизма авторизации применяется идентификатор (логин) и пароль.

2.5 Идентификатор пользователя и его пароль являются строго уникальными. Не допускается создание единых идентификаторов и паролей на несколько лиц («гостевые входы») и передача пароля другим лицам.

2.6 Пользователь несет ответственность за любую деятельность, осуществляемую с использованием его индивидуального идентификатора и пароля.

2.7 Пароль является конфиденциальной информацией. Пользователь несет ответственность за нарушение конфиденциальности своего пароля.

2.8 При вводе пароля пользователю необходимо исключать возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.).

2.9 Запрещается хранить идентификатор и пароль пользователя в доступном посторонним лицам месте.

Хранение пользователем своего пароля на бумажном носителе допускается только в запечатанном конверте.

2.10 В случае необходимости хранения паролей пользователям допускается использовать программы-менеджеры паролей (KeePass и т.п.).

2.11 Выбор паролей пользователем осуществляется с учетом следующих требований:

– пароль должен состоять не менее чем из 8 символов;

– в пароле для повышения его стойкости необходимо использовать символы неменее чем трех групп из следующих четырех:

цифры (0-9);
символы нижнего регистра (a-z, а-я);
символы верхнего регистра (A-Z, А-Я);
специальные символы (# @ +/ * и т.д.).

– пароль не должен содержать легко вычисляемые сочетания символов, например: имена, фамилии, номера телефонов, даты, последовательные расположенные на клавиатуре символы («12345678», «QWERTY», «1qaz!QAZ» и т. д.), общепринятые сокращения («USER», «TEST», «P@SSW0RD» и т.п.),

– пользователь не вправе использовать при генерации нового пароля значения предыдущих 4 паролей;

– при смене пароля значение нового должно отличаться от предыдущего неменее чем в 4 позициях;

– для различных информационных систем (далее – ИС) необходимо устанавливать собственные, отличающиеся пароли.

2.12 Продолжительность блокирования учетной записи пользователя составляет не менее 20 минут или до разблокирования учетной записи администратором.

2.13 Пользователь должен производить смену пароля не реже 1 раза в 90 дней.

2.14 Первоначально устанавливаемые пароли для каждого пользователя являются уникальными и должны быть изменены пользователем сразу же после первого входа.

2.15 В случае компрометации пароля пользователь обязан немедленно сообщить об этом в службу охраны труда и безопасности и произвести смену пароля. В случае если нет возможности самостоятельно сменить пароль, необходимо обратиться в отдел информационной безопасности.

3. Использование антивирусной защиты

3.1 В Университете используются только лицензионные антивирусные средства, управляемые централизованно.

3.2 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 (дискетах, CD, USB-накопителях, лентах и т.п.).

3.3 Пользователю категорически запрещается прерывать работу антивирусных средств.

3.4 Пользователю запрещается отключать, изменять настройки или создавать препятствия для работы антивирусных программ.

3.5 Пользователь несет ответственность за неправильные действия при обнаружении вирусов.

3.6 Пользователь АРМ обязан проводить полную проверку внешних носителей информации при подключении их к корпоративным средствам вычислительной техники.

3.7 Пользователям АРМ категорические запрещается удалять антивирусное программное обеспечение.

3.8 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник подразделения должен незамедлительно оповестить об этом службу охраны труда и безопасности.

3.9 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего руководителя, отдел информационной безопасности, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе.

4. Использование ресурсов сети «Интернет»

4.1 Доступ к публичным ресурсам сети «Интернет» организован для получения и передачи сотрудниками Университета необходимой для служебной деятельности информации. Использование сети «Интернет» в иных целях запрещено.

4.2 Университет оставляет за собой право ограничивать доступ к ресурсам сети «Интернет», содержание которых не имеет отношения к исполнению служебных обязанностей, а так же к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством, включая материалы, содержащие вредоносную, угрожающую, клеветническую, непристойную информацию, а также оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстреканию к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д. Также Университет оставляет за собой право, при наличии технической возможности, расшифровывать трафик передаваемый по корпоративным каналам связи в зашифрованном виде при помощи протоколов SSL, TLS и т.д.

4.3 Университет оставляет за собой право блокировать различные протоколы и сервисы сети «Интернет», не относящиеся к бизнес-процессам Университета, для снижения нагрузки на корпоративные каналы связи.

4.4 Вся информация о ресурсах, посещаемых сотрудниками Университета, протоколируется и при необходимости может быть предоставлена руководителям подразделений, а также руководству Университета для детального изучения.

4.5 Передача и хранение корпоративной информации при помощи файловых хранилищ (Dropbox, Google Drive и т.д.) запрещается.

4.6 Сотрудники отдела информационной безопасности при согласовании с начальником отдела по информационной безопасности имеют право блокировать доступ к различным ресурсам сети «Интернет» на основании законодательства Российской Федерации в области защиты информации.

4.7 Университет по умолчанию блокирует доступ к ресурсам сети «Интернет», которые могут прямо либо косвенно угрожать безопасности информации, либо IT-инфраструктуре Университета:

– узлы сети TOR, а также и других сетей так называемой DarkNet;

– серверы управления вредоносным ПО, о которых стало известно из открытых источников, либо при расследовании инцидентов информационной безопасности;

– почтовые серверы, рассылающие спам, либо вредоносное ПО;

– узлы бот-сетей;

– фишинговые сайты;

– ресурсы с порнографическим содержанием;

– сайты сохранения анонимности в сети;

– ресурсы, содержащие информацию преступного характера, в том числе о преступлениях в области информационных технологий;

– ресурсы, содержащие информацию, запрещенную к распространению российским или международным законодательством.

4.8 При работе с ресурсами сети «Интернет» запрещается:

– распространение защищенных авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт и прочие права собственности и/или авторские и смежные с ними права третьей стороны;

– умышленная публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, а также для осуществления несанкционированного доступа

– применять при работе в сети «Интернет» какие-либо средства сетевого анализа и мониторинга (сетевые сканеры, снифферы, и т.д.), технологии массовых рассылок почтовых сообщений (СПАМ) и иные программные средства, способные принести вред другим пользователям сети «Интернет»;

– самостоятельно устанавливать дополнительные прокси-сервера или иные программное – технические средства для скрытого доступа в сеть «Интернет»;

– осуществлять доступ в сеть «Интернет» с АРМ через модем по коммутируемому каналу связи, некорпоративным беспроводным сетям (WiFi, GPRS, EDGE и др.)

– несанкционированно выгружать конфиденциальную служебную информацию на сторонние web-ресурсы и носители.

5. Работа с бумажными носителями

5.1 Запрещается оставлять конфиденциальные документы, напечатанные на бумажном носителе, без присмотра в доступном сторонним лицам месте.

5.2 Необходимо использовать шредер для уничтожения бумажных носителей, которые содержат конфиденциальную информацию. Запрещается выбрасывать бумажные носители, которые содержат конфиденциальную информацию в мусорные корзины (урны).

6. Удаленный доступ к сети Университета

6.1. Сотруднику Университета может быть предоставлен удаленный доступ к информационно-телекоммуникационной сети.

6.2. Для оформления заявки на предоставление удаленного доступа сотруднику необходимо обратиться к проректору, курирующему направление информационной безопасности и предоставить обоснование (Приложение 1).

6.3. Запрещается использовать сторонние VPN клиенты и программы для получения удаленного доступа к ресурсам Университета.

6.4. Запрещается в рамках удаленного доступа передавать в КИС Университета вредоносное содержимое.

6.5 При удаленной работе в локальной сети Университета пользователь обязан соблюдать следующие правила:

– запрещается копировать информацию из локальной вычислительной сети Университета на удаленный компьютер (если удаленный компьютер не является собственностью Университета);

– запрещается оставлять без контроля рабочее место во время сеанса подключения, не заблокировав компьютер;

– запрещается несанкционированное изменение/уничтожение данных, или программы в локальной вычислительной сети Университета;

– запрещается использовать предоставленный доступ не по прямому назначению.

7. Ответственность

7.1 Сотрудники, нарушившие требования информационной безопасности и руководители подразделений, не обеспечившие их выполнение, несут персональную ответственность в соответствии с Трудовым договором и действующим Законодательством РФ.

7.2 К нарушителям могут быть применены меры материального и дисциплинарного воздействия, вплоть до увольнения, на основании статьи 81 Трудового кодекса РФ.

7.3 При совершении преступлений (мошенничество, диверсия, кража и прочее) материалы по ним передаются в правоохранительные органы Российской Федерации.

7.4 За разглашение (умышленное или неосторожное), а также за незаконное использование информации, составляющей коммерческую тайну, конфиденциальную информацию, служебную тайну, предусмотрена дисциплинарная, гражданско-правовая, административная и уголовная ответственность.

Приложение 1

Форма заявления на предоставление удаленного доступа к информационным ресурсам Университета

СОГЛАСОВАНО
Проректор курирующий направление ИБ «___» _____ 20__ г.

СОГЛАСОВАНО
Начальник службы охраны труда и безопасности «___» _____ 20__ г.

СОГЛАСОВАНО
Управление по работе с персоналом «___» _____ 20__ г.

СОГЛАСОВАНО
Начальник отдела информационной безопасности «___» _____ 20__ г.

ЗАЯВЛЕНИЕ № _____

Прошу предоставить удаленный доступ к информационным ресурсам Университета:

Наименование структурного подразделения	
Ф.И.О. сотрудника, должность, телефон	
Ф.И.О. непосредственного руководителя, должность, телефон	
Необходимые информационные ресурсы	

Период предоставления удаленного доступа: «___» _____ 20__г. по «___» _____ 20__г.

Обоснование служебной необходимости: *примеры – больничный лист, трудовой договор в котором указан формат работы «удаленный» и т.д.*

_____ _____ «___» _____ 20__ г.
фамилия И.О. руководителя подразделения подпись дата

С положением по соблюдению требований информационной безопасности в ФГБОУ ВО «АГУ им. В.Н. Татищева» ознакомлен(а)

_____ _____ «___» _____ 20__ г.
фамилия И.О. сотрудника подпись дата