Министерство образования Белгородской области
Областное государственное автономное профессиональное образовательное учреждение «Алексеевский колледж»
(ОГАПОУ «Алексеевский колледж»)

СОГЛАСОВАНО
Председатель первичной профсоюзной организации ОГАПОУ «Алексеевский колледж»
О. И. Пьянзина
«05» февраля 2025 г.

УТВЕРЖДЕНО
Директор ОГАПОУ «Алексеевский колледж»
О.В. Афанасьева
Приказ № 212
.«27» февраля 2025 г.

РАССМОТРЕНО
на заседании Общего собрания работников и обучающихся ОГАПОУ «Алексеевский колледж»
Протокол № 5
« 14» февраля 2025 г.

Подписано цифровой подписью: Афанасьева Ольга Валерьевна
DN: cn=Афанасьева Ольга Валерьевна, o=ОГАПОУ "Алексеевский колледж", ou=Директор, email=afanasjeva_o@alcollege.ru, c=RU
Дата: 2025.03.11 11:16:25 +03'00'

Инструкция по информационной безопасности при использовании автоматизированного рабочего места ОГАПОУ «Алексеевский колледж»

Алексеевка, 2025

I. Учётные записи и пароли пользователя

Для каждого сотрудника создаётся персональная учётная запись, в которую входят логин и пароль, это необходимо для авторизации пользователя в информационных системах. Сотрудник несёт персональную ответственность за действия, произведённые через его учётную запись.

Для защиты рабочего места и учётной записи, есть ряд правил, которые необходимо соблюдать:

– знание требований руководящих документов по защите информации;

– ознакомление сотрудников с документами по защите информации необходимо производить под подпись;

– запрещено передавать и разглашать персональные учётные записи, пароли и электронные идентификаторы;

– запрещено пользоваться чужими учётными записями и паролями;

– необходимо использовать «сложные» пароли и производить их замену
раз в 3 месяца;

– запрещено хранить пароли в доступных местах (блокнот, монитор, коврик для мыши, клавиатура и т. д.);

– автоматизированное рабочее место (далее – АРМ) не должно оставаться без присмотра, так как за сохранность информации отвечает сам сотрудник. При оставлении без присмотра АРМ необходимо заблокировать сеанс операционной системы. В большинстве отечественных операционных систем для блокировки сеанса работает сочетание клавиш Alt+Ctrl+L;

– при утере пароля и электронного идентификатора или невозможности войти в учётную запись под своим паролем, необходимо немедленно сообщить об этом техническому специалисту;

– разрешено хранить личный пароль в запечатанном конверте в сейфе у руководителя структурного подразделения или его заместителя.

1.1. Требования в отношении паролей:

Пароли должны выбираться пользователями АРМ самостоятельно с учётом следующих требований:

1. Длина пароля должна быть не менее 8 символов.

2. В числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.д.).

3. Пароль должен вводиться в режиме латинской раскладки клавиатуры.

4. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.д.).

5. Запрещается использовать в качестве пароля имя входа в систему,

простые пароли типа «123», «111», «qwerty» и им подобные, а также имя и дату рождения (свои и своих родственников), клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о сотруднике.

6. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

7. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т. п.).

8. Запрещается выбирать пароли, которые уже использовались ранее.

9. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

10. Личный пароль сотрудник не должен сообщать никому.

11. Полная смена паролей пользователей должна проводиться регулярно не реже одного раза в квартал во всех информационных системах, к которым сотрудник имеет доступ.

12. Контроль за действиями сотрудника при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на сотрудников и руководителей, ответственных за информационную безопасность.

13. Внеплановая смена личного пароля или удаление учётной записи сотрудника АРМ производится владельцем системы после его уведомления руководителем структурного подразделения увольняемого сотрудника или сотрудником, назначенным ответственным за информационную безопасность в орган (организации).

1.2. Смена пароля в СЭД «Мотив»

Для самостоятельной смены пароля в системе Электронного правительства Белгородской области необходимо предпринять следующие шаги:

1. Перейти на сайт по ссылке: https://pbo.belregion.ru/login.

2. В окне ввода данных нажать на «Забыли пароль?»

Далее в окне восстановления пароля ввести адрес корпоративной электронной почты, куда придет письмо со ссылкой для восстановления пароля.

4. Перейти по ссылке из письма и ввести новый пароль.

Требования к паролю системы Электронного правительства Белгородской области аналогичны требованиям, перечисленным в п.1.1

1.3. Смена пароля учётной записи в Белгородской Единой Системе Авторизации

Для самостоятельной смены пароля учётной записи необходимо предпринять следующие шаги:

1. Перейти на сайт по ссылке: https://login.belregion.ru, ввести логин и пароль и осуществить вход в Личный кабинет.

2. Перейти во вкладку «Безопасность» – «Пароль» и задать значения для смены пароля.

3. Нажать «Сохранить».

Требования к паролю учетной записи аналогичны требованиям, перечисленным в п.1.1.

II. Правила использования сети Интернет

Работа в сети Интернет должна проводится сотрудником для исполнения должностных обязанностей с обязательно включёнными средствами защиты информации.

Использовать сеть Интернет для повышения профессиональной квалификации.

Обмен сообщениями и документами между сотрудниками осуществлять только с использованием корпоративной электронной почты.

В сети Интернет запрещено:

– Работать при выключенных средствах защиты (обязательное использование антивирусного программного обеспечения);

– скачивать из сети Интернет программное обеспечение и другие файлы, которые могут нанести вред вашему оборудованию (торренты, файлы с раширением «.exe, .rar» и т. п.);

– посещать сайты, не связанные с должностными обязанностями (социальные сети, интернет-магазины, сервисы потокового видео), а также размещать на них служебную информацию;

– пользоваться личной электронной почтой для служебных сообщений, расположенной на бесплатных почтовых сервисах (gmail.com, outlook.com, yahoo.com, tuta.com, mailfence.com, @protonmail.com и др.)

– использовать игровые сервисы и приложения, torrent-клиенты, утилиты и программы для удаленного администрирования АРМ и серверов;

– использовать и размещать служебную информацию на иностранных сервисах, таких как google и др., а также в чат-ботах и инструментах с элементами искусственного интеллекта.

III. Правила использования электронной почты

Электронная почта предоставляется сотрудникам только для исполнения своих служебных обязанностей.

При пользовании электронной почтой строго запрещено:

1. Использование её в личных целях.

2. Пересылать информацию ограниченного доступа (персональные данные, информацию для служебного пользования).

3. Пересылать нелегально распространяемые материалы (аудио - и видеоданные, программное обеспечение, письма с сомнительными

вложениями, такими как поздравительные открытки, подарочные карты, сертификаты на приобретение товаров и т. п.).

4. Указывать служебные электронные адреса в общедоступных ресурсах сети Интернет (блоги, форумы и т. п.), если это не связано со служебной необходимостью.

5. Производить рассылку материалов рекламного (непрофильного) и развлекательного характера;

6. Производить массовую рассылку писем непроизводственного характера;

7. Пересылать исполняемые файлы (с расширениями – .exe, .dll, .pif и т. п.);

8. Пересылать мультимедийные файлы (аудио и видео);

9. Производить рассылку вредоносных программ или файлов, заражённых вирусами;

10. Переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные, или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т. д.);

11. Нажимать на ссылки из писем, если они заменены на слова, наводить на них курсор и просматривать полный адрес сайта;

12. Открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, файлы с расширениями: RTF, LNK, CHM, VHD;

13. Открывать письма от неизвестных адресатов;

14. Осуществлять деятельность, нарушающую законы и нормативные правовые акты Российской Федерации;

15. Предоставлять кому-либо логин и пароль для доступа к своей корпоративной электронной почте.

IV. Установка программного обеспечения на АРМ

В технических средствах АРМ необходимо использовать только лицензионное программное обеспечение фирм-изготовителей, полученное из доверенных источников. Приоритет ставить на отечественное программное обеспечение в рамках импортозамещения.

При установке дополнительного программного обеспечения необходимо согласовать с техническим специалистом, ответственным за информационную безопасность возможность его использования, после чего направить соответствующую заявку в службу поддержки пользователей «Service Desk» (Рис. 4), ссылка для перехода: https://help.belregion.ru

Сотрудник в части касающейся обязан знать порядок эксплуатации программного обеспечения и уметь правильно его применять в ходе исполнения должностных обязанностей.

Ознакомление и обучение сотрудников работе с программным обеспечением в пределах выполняемых функций проводит сотрудник подразделения, ответственного за сопровождение информационной системы,

ресурса, средства защиты информации.

Необходимо исключить попадание в систему средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.

В случае обнаружения программного обеспечения, не входящего в список доверенных программ и не предназначенного для выполнения служебных обязанностей, сотрудник обязан немедленно прекратить работу и проинформировать технического специалиста или сотрудника, назначенных ответственными за информационную безопасность в организации, при необходимости направить заявку в службу поддержи на удаление вышеуказанного программного обеспечения.

При установке программного обеспечения необходимо назначать минимально необходимые права и привилегии пользователям и лицам, выполняющим обработку служебной информации.

V. Правила пользования антивирусной защитой

В целях защиты информации от вредоносных программ на автоматизированном рабочем месте устанавливается антивирусное программное обеспечение Dr.Web., которое настроено администратором для осуществления эффективной антивирусной защиты (обновление антивирусных баз и сканирование операционной системы происходит в автоматическом режиме по заранее запланированному графику, настройки политики безопасности также находятся под управлением администратора, не пытайтесь настроить антивирус Dr.Web самостоятельно!

Для проверки файла или папки с файлами нужно выполнить ряд действий:

1. Открыть интерфейс антивируса Dr.Web, в окне появится сообщение

«Перетащите сюда файлы или нажмите для выбора», перетащите файл для проверки (осуществите его выбор), после чего начнётся проверка.

2. Зайти в папку, где расположен файл или папка с файлами, нажать правой кнопкой мыши по имени проверяемого файла или папки с файлами. После этого высветится меню, где нужно выбрать пункт «проверить Dr.Web».

3. В раскрывшемся окне он начинает проверять файл или папку с файлами на наличие угроз.

4. По окончании сканирования в окне отображается результат проверки с указанием обнаруженных объектов и угроз.

5. В случае обнаружения сканером угроз, он предложит их обезвредить, для этого необходимо нажать кнопку «обезвредить».

6. В случае обнаружения вредоносного программного обеспечения на АРМ не поддающегося лечению антивирусной программой, пользователь обязан немедленно поставить в известность ответственного за информационную безопасность и руководителя структурного подразделения,

прекратить обработку информации на АРМ и направить в обязательном порядке соответствующую заявку в службу поддержки. В свою очередь ответственный за информационную безопасность должен убедиться в актуальности используемых антивирусных баз и уведомить отдел информационной безопасности департамента инфраструктурных решений министерства цифрового развития Белгородской области о выявленных фактах. Работа на АРМ запрещается до решения вопроса о возможности дальнейшей его эксплуатации.

В процессе своей работы Dr.Web автоматически проверяет все сообщения электронной почты, проходящие через сервер. При этом проверяются файлы вложений, а также все объекты OLE, встроенные в документы. При обнаружении вирусов в почтовом сообщении тело вируса изымается и перемещается в зону карантина, после чего администратору сервера приходит извещение.

Также при получении подозрительных сообщений и файлов по электронной почте сотрудник может обратиться в службу поддержки для проверки и оценки файла на предмет угроз безопасности информации, либо перенаправить сообщение на электронный почтовый ящик (avz@belregion.ru), где будет проведена проверка сообщения на предмет угроз информационной безопасности.

VI. Обращение с ключевой информацией электронной подписи

При использовании электронной подписи (далее - ЭП) необходимо соблюдать следующее:

– хранить в тайне ключ ЭП;

– не использовать для ЭП и шифрования ключи, если известно, что эти ключи используются или использовались ранее;

– использовать ключ ЭП только на рабочем месте и не передавать его третьим лицам;

– немедленно требовать приостановления действия сертификата ключа проверки ЭП при наличии оснований полагать, что тайна ключа ЭП (закрытого ключа) нарушена (произошла компрометация ключа);

– обновлять сертификат ключа проверки ЭП в соответствии с установленным регламентом;

– хранить электронную подпись только на специальных ключевых носителях, таких как: Rutoken, E-token, E-smart USB, JaCarta LT, JaCarta-2 SE.

Ключевой носитель должен быть зарегистрирован в журнале учёта идентификаторов, храниться в служебном сейфе в запечатанном конверте. В случае отсутствия условий для хранения у сотрудника, ключевой носитель должен храниться в сейфе руководителя структурного подразделения в запечатанном виде.

В случае утери ключевого носителя (контейнера) необходимо уведомить технического специалиста или ответственного за

информационную безопасность в органе (организации), а также руководителя структурного подразделения, принять меры по отзыву сертификата ЭП посредством перехода на портал заявителя удостоверяющего центра Федерального казначейства fzs.roskazna.ru Рис. 8 и оформления заявки на прекращение действия сертификата.

При необходимости на портале заявителя в установленном порядке сотрудник может подать заявку для получения нового сертификата ключа ЭП.

VII. Правила пользования БелОфис

При использовании облачного сервиса БелОфис необходимо руководствоваться инструкциями.

При совместном использовании необходимо жёсткое ограничение круга лиц, имеющих право доступа к документу, при этом в дополнительных параметрах доступа необходимо проставить «галочки» (Нельзя распечатать, скачать и скопировать файл (для доступа Только чтение и Комментирование), Нельзя менять настройки доступа (для Полного доступа).

Категорически запрещено активировать копирование внешней ссылки.

В случае активности копирования внешней ссылки её необходимо выключить.

Категорически запрещена обработка персональных данных в БелОфис.

VIII. Социальная инженерия

Киберпреступники всё чаще используют методы социальной инженерии для проникновения в инфраструктуру бюджетных организаций и органов власти.

Человеческий фактор по-прежнему остается слабым звеном в любой системе защиты, поэтому пользователям необходимо знать основы информационной безопасности.

Убеждайтесь в подлинности личности лица, звонящего по телефону или контактирующего с иным способом, а также в правомочности его запросов.

Не предоставляйте никакой информации при первом контакте, а лично инициируйте повторный контакт.

Сохраняйте бдительность. Всегда проверяйте уровень конфиденциальности

информации перед ее передачей контактирующему с Вами лицу и наличие у него права на доступ к ней. Если есть сомнения, свяжитесь с техподдержкой или представителем организации контактирующего по официальным каналам.

Ознакомьтесь с практиками социальной инженерии и не поддавайтесь им. При получении писем по электронной почте необходимо проверять адресат на предмет подлога, web-подделки, и принадлежности к фишинговым ссылкам; не переходить по сомнительным ссылкам и т. п.

Внимательно проверяйте ссылки, даже если письмо получено от другого пользователя информационной системы.

Обычно злоумышленники пытаются сделать свои письма предельно нейтральными, чтобы минимизировать количество признаков, по которым можно отличить фальшивое сообщение от настоящего. Если письмо выглядит правдоподобно, но вы всё равно сомневаетесь, не стесняйтесь обратиться за помощью к сотруднику, ответственному за информационную безопасность в органе (организации), или переслать его на почтовый ящик avz@belregion.ru.

В случае если вы всё-таки попались на уловку злоумышленников, то как можно скорее сообщите об этом сотруднику или руководителю, назначенным ответственными за информационную безопасность в организации.

IX. В процессе работы сотруднику запрещается:

– оставлять без личного контроля свой персональный идентификатор, пароль и передавать его другим лицам;

– использовать недокументированные свойства и ошибки в программном обеспечении или в настройках технических средств, которые могут привести к возникновению нештатных ситуаций;

– самостоятельно вносить изменения в состав, конструкцию, конфигурацию и размещение технических средств АРМ;

– производить модификацию, уничтожение и блокирование общего и специального (прикладного) программного обеспечения, применяемого для обработки информации;

– осуществлять попытки несанкционированного доступа к информационным ресурсам АРМ;

– отключать (блокировать) средства защиты информации АРМ;

– использовать неисправные машинные носители информации (далее – МНИ) для её хранения и обработки;

– использовать неучтённые МНИ;

– разглашать сведения о реализованном на АРМ комплексе средств защиты информации (антивирусное программное обеспечение, средства криптографической защиты и т. п.);

– оставлять АРМ при выходе из помещения, в котором оно установлено, не убедившись, что оно заблокировано, или отключено.

Важно знать! Информация, содержащая сведения, составляющие государственную тайну, а также иная информация ограниченного доступа должна обрабатываться на АРМ, аттестованных на соответствие требованиям о защите информации. Обработка информации ограниченного доступа, в том числе составляющей государственную тайну, на АРМ, не предназначенных для её обработки, влечёт за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

X. Сотрудник обязан:

– немедленно докладывать техническому сотруднику или ответственному за информационную безопасность в организации, а также руководителю структурного подразделения о выявленных изменениях в конфигурации технических средств и программного обеспечения АРМ, о фактах и попытках несанкционированного доступа к обрабатываемой информации на АРМ, о возникновении нештатных ситуаций, связанных с использованием АРМ, таких как:

– подозрения компрометации (разглашения, утечки, несанкционированного копирования или использования) личных паролей или закрытых ключей, применяемых для входа в АРМ;

– подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках);

– несанкционированные (произведенных с нарушением установленного порядка) изменения в конфигурации программных или аппаратных средств;

– отклонения в нормальной работе системного и прикладного программного обеспечения, затрудняющие эксплуатацию АРМ;

– обнаружение ошибок в программном обеспечении или в настройках технических средств АРМ;

– некорректное функционирование установленных на АРМ средств защиты информации.

ВАЖНО ЗАПОМНИТЬ!!!

При возникновении проблем, связанных с эксплуатацией АРМ, таких как неисправная работа периферийных устройств, организационной техники (мышь, клавиатура, монитор, системный блок, принтер, МФУ, сетевое подключение и т.п.), при сбоях в работе операционной системы, программного обеспечения, возникновении ошибок авторизации и иных отклонениях в нормальной работе АРМ пользователь обязан уведомить об этом руководителя структурного подразделения и подать заявку в службу поддержки для устранения выявленных недостатков.

Не пытайтесь решить проблему самостоятельно (осуществить ремонт или настройку АРМ)!!! Это запрещено и влечёт персональную ответственность сотрудника в соответствии с действующим законодательством Российской Федерации.

XI. Ответственность за неисполнение данных правил:

Сотрудник несёт персональную ответственность за ненадлежащее исполнение своих обязанностей, а также сохранность комплекта АРМ, МНИ, электронных идентификаторов и целостность установленного программного обеспечения.

Ответственность за нарушение функционирования АРМ или его компонентов, уничтожение, блокирование, несанкционированные операции копирования и распространения, а также модификации и замены

информации, обрабатываемой на АРМ, несёт сотрудник, идентификационные данные которого были использованы при совершении нарушения.

Сотрудники, виновные в нарушениях, несут ответственность в соответствии с действующим законодательством Российской Федерации.