Утверждаю:

Директор

_____ /Кузнецов С.А. /

«03» апреля 2023 г.

ИНСТРУКЦИЯ

по защите персональных данных (конфиденциальной информации) в Профессиональном образовательном учреждении частном «Колледж менеджмента»

1. Общие положения

1.1. Целью настоящей инструкции является четкая регламентация эффективных мер защиты и надежного сохранения информации согласно Политики информационной безопасности (Политики обработки персональных данных) (далее - Политики) в ПОУЧ «Колледж менеджмента» (далее - Учреждение) и обрабатываемой в автоматизированной системе (далее - АС). Мероприятия защиты проводятся для обеспечения физической и логической целостности, а также для предупреждения несанкционированного получения, распространения и модификации информации. Меры защиты подразумевают обязательное наличие ответственного за защиту информации в АС лица, выработку и неукоснительное соблюдение организационных мер.

1.2. Термины и определения

Авторизованный субъект — субъект АС, пользовательские функции которого, а также права и обязанности по отношению к данного уровня ресурсам и информации определены его должностной инструкцией, либо другими административными актами.

АРМ — автоматизированное рабочее место, персональное, созданное на основе персональной электронной вычислительной машины.

Доступность ресурса — обеспечение беспрепятственного доступа к нему авторизованного субъекта АС.

Конфиденциальность ресурса - свойство ресурса быть доступным только авторизованному субъекту АС, и одновременно быть недоступным для неавторизованного субъекта или нарушителя.

Ресурс — компонент АИС (аппаратные средства, программное обеспечение, данные), в отношении которого необходимо обеспечивать безопасность, т. е. конфиденциальность, целостность и доступность.

Субъекты АС — пользователи, технический персонал, обеспечивающий работу системы, администрация АС, администрация Учреждения и контролирующие службы.

Целостность ресурса — обеспечение его правильности и работоспособности в любой момент времени.

2. Допуск к использованию ресурсов

Допуск к работе с конфиденциальными документами (конфиденциальной информацией) имеют сотрудники Учреждения, в том числе и находящиеся на испытательном сроке, которые: ознакомлены под роспись с Политикой Учреждения,

настоящей Инструкцией, другими организационно-распорядительными документами; подписали Соглашение о неразглашении персональных данных (конфиденциальной информации).

Запрещается допускать к работе с конфиденциальными документами (персональными данными) других лиц, кем бы они не являлись, без письменного разрешения руководителя Учреждения.

Под допуском подразумевается официальное присвоение сотруднику Учреждения конкретного статуса, дающего ему возможность использовать ресурсы АС и обмена данными на заданном четко категорированном уровне и в ограниченном должностными обязанностями (не превышающем его непосредственные задачи) объеме.

Обязанности по присвоению статуса возлагаются на ответственного за защиту персональных данных (Администратора автоматизированной системы, локальной сети, объекта информатизации и т.п.) или специально назначенного сотрудника. При этом он должен, руководствоваться принципами разумного ограничения возможностей и разграничения доступа к различным информационным массивам. Он несет ответственность за регистрацию и предоставление (изменение) полномочий.

Все пользователи подлежат учету по категориям установленного допуска и другим системным параметрам.

3. Доступ к использованию ресурсов. Регистрации пользователей

Доступ к использованию ресурсов имеют сотрудники, получившие допуск определенного уровня, соответствующий, как правило, занимаемой должности, с соблюдением всей процедуры оформления допуска, и зарегистрированные у Администратора (Ответственного должностного лица).

3.1. Специальные вопросы доступа к использованию ресурсов:

3.1.1. Определение расширенного доступа, т. е. привилегий системного Администратора.

Привилегии Администратора, кроме тех сотрудников, которым должностными обязанностями предписано выполнять работы по эксплуатации и ремонту ресурсов, имеют право получать представители руководства Учреждения и другие должностные лица по согласованию со специально назначенным сотрудником и с разрешения руководителя Учреждения. Все лица, имеющие права Администратора, подлежат отдельному учету.

3.1.2. Доступ к работе с авторским (лицензионным) программным обеспечением (далее - ПО).

При наличии в АС или ее компонентах авторских либо лицензионных программ они должны быть соответствующим образом, ясным для пользователя, помечены; там же должны быть указаны все ограничения, связанные с работой с данным Г10.

Однозначно (но умолчанию) запрещается их копирование.

4. Хранение носителей персональных данных (конфиденциальной информации) в АС

За организацию хранения и сохранность персональных данных (конфиденциальной информации) Учреждения отвечает его руководитель. Контроль за выполнением мероприятий осуществляет Ответственный за обработку персональных данных (далее — ПДн) (защиту информации). Общий процесс хранения регламентирован в локальных актах Учреждения.

Машинные носители персональных данных (конфиденциальной информации)

хранятся в недоступном для посторонних лиц месте (сейф, металлический шкаф, файл-бокс), исключающем несанкционированный доступ и пользование ими.

Сейф (-ы) (несгораемый металлический шкаф) должен быть постоянно закрыт на ключ.

Один комплект ключей от сейфа(-ов) — у ответственного сотрудника Учреждения. Остальные комплекты должны храниться в сейфе ответственного за обработку персональных данных (защиту информации) (далее - Ответственного) в опечатанном (или иным способом обеспечивающим целостность) пенале. Порядок опечатывания и сдачи, под охрану сейфов определяется локальными актами Учреждения.

5. Защита ресурсов АС

5.1. В целях обеспечения надежной охраны материальных ценностей вычислительных средств, сетей и данных конфиденциального характера, своевременного предупреждения и пресечения попыток несанкционированного доступа к ним устанавливается определенный режим деятельности, соблюдение которого обязательно для всех сотрудников, посетителей и клиентов. Порядок его регламентации устанавливается в локальных актах Учреждения.

При этом: запрещен несанкционированный внос-вынос машинных накопителей информации (дискет, CD-R, USB накопителей, переносных накопителей на твердых магнитных дисках и т.п.); запрещено кому бы то ни было, кроме специально уполномоченных сотрудников, перемещать компьютерную технику и комплектующие без соответствующих сопроводительных документов (служебных записок или накладных), согласованных с Ответственным.

5.2. Аппаратная защита ресурсов проводится исходя из потребностей Учреждения в реальном сохранении своей информации ограниченного доступа по назначению руководства и может включать в себя:

- использование источников бесперебойного или автономного питания;
- поддержание единого времени;
- изъятие с АРМов необязательных дисководов, факсимильных и модемных плат и т.п.;
- проведение периодических «чисток» АРМов и общих системных директорий на файл- серверах и серверах АС.

5.3. Программная защита ресурсов также проводится исходя из потребностей Учреждения в реальном сохранении своей информации ограниченного доступа по назначению руководства и может включать в себя:

- установку входных паролей на клавиатуру АРМ;
- установку сетевых имен-регистраторов и паролей для доступа к работе в АС;
- обеспечение восстановления информации после несанкционированного доступа;
- обеспечение антивирусной защиты (в т. ч. от неизвестных вирусов) и восстановления информации, разрушенной вирусами;
- контроль целостности программных средств обработки информации;
- проведение периодической замены (возможно принудительной) всех паролей и регистрационных имен;
- использование расширенных систем аутентификации.

5.4. Техническая защита ресурсов включает в себя защиту АРМ, помещений и всех коммуникаций от устройств съема и передачи информации.

6. Копирование персональных (конфиденциальных) данных

Согласно Политике Учреждения копирование информации (персональных данных) запрещено, если это не оговорено дополнительно, т.е. запрещено копирование в любые другие, несанкционированные виртуальные области и на прочие носители. Порядок получения разрешения на копирование определен локальными актами Учреждения.

7. Архивирование персональных данных (конфиденциальной информации)

Архивирование текущей конфиденциальной информации (персональных данных) в АС проводится пользователями не реже чем один раз в неделю. Архивирование должно также предусматривать восстановление разрушенной архивной информации, даже при ее значительных потерях. С этой целью делаются ежедневные, еженедельные и т. д. архивные копии. Копии на твердых носителях архивируются и хранятся согласно Политики Учреждения.

8. Уничтожение данных, содержащих персональные данные (конфиденциальную информацию)

Процесс создания конфиденциальных документов и обработки данных в АС после получения печатных и прочих копий для дальнейшей работы должен при необходимости завершаться очисткой памяти и рабочих областей на машинных носителях. Для уничтожения персональных данных (конфиденциальной информации) назначается специальная комиссия. Уничтожения информации проводится согласно Инструкции с составлением Акта.

9. Передача персональных данных (конфиденциальной информации)

Порядок передачи персональных данных (конфиденциальной информации) на различных носителях регламентируется должностными инструкциями, а также Политикой.

Все факты получения информации должны быть надежно подтверждены.

На Ответственного также возлагаются обязанности по правильному управлению потоками данных с целью предотвращения записи персональных данных (конфиденциальной информации) на посторонние носители информации.

10. Доведение специальных правил обращения с персональными данными (конфиденциальной информацией) в АС до персонала

Доведение данной инструкции до персонала проводится ответственным или руководителем Учреждения при ознакомлении сотрудника с Политикой. Повторное ознакомление и разъяснение данной Инструкции проводится специально назначенным ответственным лицом Учреждения при предоставлении доступа, за что сотрудник расписывается в графе «Ознакомлен» журнала ознакомления или в ином локальном документе Учреждения, например: «Журнале учета доведения нормативных документов».

Все изменения и дополнения настоящей Инструкции официально доводятся до всего персонала (сотрудников) Учреждения.

11. Защита персональных данных (конфиденциальной информации) пользователями ресурсов

Пользователь лично отвечает за понимание и соблюдение правил безопасности. Если ему не понятны функции по защите информации он обязан спросить Ответственного. Запрещаются любые действия, направленные на:

- получение доступа к информации о пользователях;
- вскрытие и использование чужих регистрационных имен (логинов) и паролей;
- тестирование и разрушение служб сети;
- просмотр всех доступных для чтения файлов на сетевых устройствах не принадлежащих пользователю;
- модификация файлов, которые не являются собственными, даже если они имеют право записи в них;
- вскрытие блоков и комплектующих, а также изменение физической конфигурации;
- использование одного и того же регистрационного имени и пароля;
- раскрывание и передача кому бы то ни было своего регистрационного имени и(или) пароля.

При выборе пароля Пользователь **обязан:**

- не использовать регистрационное имя в каком бы то ни было виде;
- не использовать имя, фамилию или отчество в каком бы то ни было виде, имена супруга или детей, а также другую информацию, которую легко получить (номер телефона, дату рождения и пр.);
- не использовать пароль из одних цифр или их одних букв, а также короче шести символов;
- использовать пароль с буквами из разных регистров, с небуквенными символами;
- использовать пароль, который легко запомнить, чтобы не возникало желания записать его, а также который можно легко набрать на клавиатуре, не глядя на нее.

Пользователю при работе с персональными данными (конфиденциальной информацией) **запрещено,** отлучаясь из помещения, оставлять свой АРМ без блокировки операционной системы (рабочего стола). Рабочие файлы и базы данных, содержащие конфиденциальную информацию, пользователь обязан хранить в установленных местах.

В целях выявления незаконного использования регистрационного имени Пользователь должен контролировать свое время входа и выхода в АС и проверять последние команды и, если параметры отличаются, обязан немедленно сообщить об этом Ответственному (Администратору).

Пользователь обязан немедленно сообщать о возникших проблемах и ошибках, которые не могут быть устранены путем перезагрузки компьютера после отключения от системных служб. Производить любые попытки восстановления работы компьютера при наличии соединения с системой **категорически запрещается.**

12. Ответственность за нарушение правил обращения персональных данных (конфиденциальной информации) в АС

За умышленное невыполнение или халатное исполнение правил обращения с персональными данными (конфиденциальной информацией), изложенных в данной Инструкции, если это повлекло за собой нанесение материального ущерба, виновное лицо наказывается в административном (дисциплинарном) порядке. Размер и кратность возмещения ущерба определяется в соответствие с законодательством **РФ,** после проведения внутреннего расследования.

По итогам проведения внутреннего расследования инцидентов информационной

безопасности, руководителем Учреждения могут быть инициированы ходатайства в надзорные органы о возбуждении уголовного или гражданского судебного делопроизводства.

13. Контроль

Контроль за выполнением требований Настоящей Инструкции сотрудниками и работниками Учреждения возлагается на Руководителя Учреждения и Ответственного.