Общеобразовательная автономная некоммерческая организация
«Классическая Православная гимназия святого праведного Иоанна Кронштадтского»
143988 Московская область, г.о. Балашиха, мкр. Павлино, д. 13
e-mail: melnichuk-52@mail.ru, тел. (495) 527-48-40 сайт: www.klass-gim.ru
ОКПО 81719687, ОГРН 1165000053866, ИНН/КПП 5012092703/501201001

УТВЕРЖДАЮ
Директор ОАНО КПГСПИК
В.М. Мельничук
«05» июня 2020 г.

ИНСТРУКЦИЯ

по защите персональных данных (конфиденциальной информации)
в ОАНО КПГСПИК

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 ОАНО КПГСПИК (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 ПО.

Однозначно (по умолчанию) запрещается их копирование.

В АС ОАНО КПГСПИК установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

- определены типы учетных записей: Пользователь, Опытный Пользователь, Администратор, Гость.

- заведение учетных записей для всех сотрудников и верификация сотрудников; заведение, активация, блокирование и уничтожение учетных записей пользователей, в том числе временных; пересмотр и, при необходимости, корректировка учетных записей пользователей проводится ответственным лицом ОАНО КПГСПИК с периодичностью не реже чем 1раз в 90 дней. Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования АС, для организации гостевого Доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным Доступом к информационной системе).
- предоставление пользователям прав доступа к объектам доступа АС, основываясь на задачах, решаемых пользователями в АС и взаимодействующими с ней информационными системами.
- уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе.

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-регйстраторов 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. Правила и процедуры идентификации и аутентификации

В информационной (автоматизированной) системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

Идентификация устройств в информационной (автоматизированной) системе обеспечивается по логическим именам (имя устройства и (или) Ю) логическим адресам (например, 1Р'адресам) и (или) по физическим адресам (например, МАС-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

Идентификация Wifl-Router, используемого в составе локальной сети АС ОАНО КПГСПИК, организуется в целях исключения подмены устройств беспроводного доступа обеспечивающих доступ АС к сети «Интернет».

В АС ОАНО КПГСПИК установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в АС:

- определено должностное лицо (администратор) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств (не определено);
- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству; блокирование идентификатора пользователя после установленного оператором времени неиспользования.

В АС ОАНО КПГСПИК механизм аутентификации для пользователей реализован на основе пароля, установлены следующие минимальные характеристики пароля:

- Для пользователей с правами Администратора: длина пароля не менее шести символов; алфавит пароля не менее 60 символов; максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток; блокировка АРМ или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут; смена паролей не более чем через 120 дней.

Для пользователей с правами Пользователя и (или) Опытного Пользователя:

- длина пароля не менее шести символов; алфавит пароля не менее 30 символов; максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток; блокировка АРМ или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут; смена паролей не более чем через 180 дней.

7. Копирование персональных (конфиденциальных) данных согласно Политики 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.

8. 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.

9. 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. Уничтожение информации проводится согласно Инструкции с составлением Акта.

Пользователями должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

Применяются следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

а) удаление файлов штатными средствами операционной системы и (или) форматирование машинного носителя информации штатными средствами операционной системы;

б) перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

10. 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.

11. 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.

12. Защита информационной. системы, ее средств, систем связи и передачи данных

Оператором обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Защита каналов связи обеспечивается путем применения средства криптографической защиты информации VipNet Client.

На объектах информационной инфраструктуры ОАНО КПГСПИК используются средства беспроводной связи WiFi.

Организованная защита с помощью беспроводных соединений включает:

ограничение на использование в информационной системе беспроводных соединений (802.11xWi-Fi,), к беспроводным устройствам подключены только АРМ, Пользователям которых доступ необходим для выполнения ими своих обязанностей;

доступ к параметрам (изменению параметров) настройки беспроводных соединений имеют только администраторы; реализация беспроводных соединений осуществляется через контролируемые интерфейсы; исключена возможность установления беспроводных соединений из-за пределов контролируемой зоны.

13. 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.

На объектах ОАНО КПГСПИК установлена система внутреннего видеонаблюдения. Доступ к терминалу осуществляется посредством идентификации/аутентификации представленных парой Логин/Пароль. Периодическая замена паролей - смена паролей проводится в срок не более чем через 90 дней.

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.

14. Регистрация событий безопасности

Оператором определены события безопасности в информационной системе, подлежащие регистрации, и сроки их хранения.

Регистрация событий безопасности производится с помощью служб операционной системы осуществляющих аудит событий безопасности. Для аудита АРМ настроены следующие события:

вход (выход) в информационную систему и загрузки (останова) операционной системы; подключение машинных носителей информации; запуск (завершение) программ и процессов (заданий, задач); попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа; попытки удаленного доступа.

К защищаемым объектам доступа относятся системные службы, файлы и каталоги.

На АРМ информация о события безопасности обеспечивает возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы учитывается дата и время входа (выхода)

в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

При регистрации подключения машинных носителей информации учитывается дата и время подключения машинных носителей информации логическое имя (номер) и тип подключаемого машинного носителя информации.

При регистрации запуска (завершения) программ и процессов (заданий, задач) учитывается дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам учитывается дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

При регистрации попыток удаленного доступа к информационной системе состав и содержание информации учитывается дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства). Предусмотрено:

возможность выбора Администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в соответствии с мерой защиты информации РСБ. ; генерация (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с мерой защиты информации РСБ.1 с составом и содержанием информации, определенными в соответствии с мерой защиты РСБ.2.

Объем памяти для хранения информации о событиях безопасности выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с РСБ.1, составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с РСБ.2, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с РСБ. 1.

На АРМ меры защиты информации о событиях безопасности включают в себя:

разграничением доступа пользователей АРМ к журналам аудита; разграничением прав доступа к механизмам настроек аудита событий.

Полный доступ к журналу событий аудита предоставлен только пользователям привилегированных учетных записей «Администратор»

15. 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.

16. Обеспечение доступности персональных данных

Оператором установлено, что периодическое резервное копирование информации проводится не реже чем раз в неделю на машинные носители информации пользователями АРМ.

Копированию подлежит информация обрабатываемая пользователями в ходе своей повседневной деятельности при выполнении ими своих служебных задач.

Хранение машинных носителей информации осуществляется в металлическом шкафу, расположенном в помещении АРМ «кадры».

Доступ к местам хранения МНИ ограничен.

Оператором обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

Восстановление информации с резервных машинных носителей информации (резервных копий) предусматривает:

восстановление обрабатываемых данных в течение 3 часов при необходимости восстановления полного объема и 1 часа при необходимости восстановления части данных.

регистрацию событий, связанных с восстановлением информации с резервных машинных носителей информации в «Журнале учета нарушений порядка обработки персональных данных».

17. Контроль

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

Ответственный за обработку персональных данных Г.И. Антонова