УТВЕРЖДАЮ
Директор МБОУ
«Средняя школа №7»
_____Гилязова И.А.
«7» ноября 2016 года

Инструкция пользователя в части обеспечения безопасности информации

1. Назначение и область действия документа

1.1. В настоящем документе определяются права, обязанности, а также ответственность пользователей государственной информационной системы Камчатского края "Сетевой город" (сегмент 072) (далее – ГИС) МБОУ «Средняя школа №7» (далее – Учреждение) в части обеспечения безопасности информации.

1.2. Все пользователи, допущенные к работе в ГИС, должны быть ознакомлены с настоящей инструкцией под роспись.

1.3. Методическое руководство работой пользователя осуществляется лицом, ответственным за организацию обработки персональных данных в ГИС.

2. Обязанности и права пользователей

2.1. Пользователь обязан:

2.1.1. Соблюдать правила «чистого стола»:

2.1.1.1. На рабочем столе персонального компьютера (далее - ПК) должны находиться только те документы (на материальных носителях), которые необходимы для выполнения пользователем должностных обязанностей в настоящий момент времени;

2.1.1.2. Документы, содержащие информацию ограниченного доступа, по завершению работы с ними и в нерабочее время должны быть убраны в надежно запираемый шкаф (хранилище) или сейф;

2.1.1.3. При выходе из-за рабочего места рабочий стол ПК пользователя должен быть заблокирован (комбинация клавиш <Win>+<L> или <Ctrl>+<Alt>+<Del> и выбрать опцию <Блокировка>);

2.1.1.4. Размещать экран монитора таким образом, чтобы исключить несанкционированный просмотр информации с него.

2.1.2. Использовать в работе «сложные» пароли. С использованием:

2.1.2.1. Верхнего и нижнего регистров;

2.1.2.2. Комбинации букв и цифр;

2.1.2.3. Пароля длиной не менее 6 символов;

2.1.2.4. Пароля, не имеющего смысловую нагрузку (например: пароль – «Lj,hj1» в русской раскладке «Добро1»), или не являющимся общераспространенной комбинацией клавиш (например, Qwerty1234, Asdasd123 и т.п.);

2.1.3. При обнаружении вируса или подозрении на вирусное заражение:

2.1.3.1. Приостановить работу на своем компьютере;

2.1.3.2. Сообщить администратору информационной безопасности (далее – Администратор ИБ) информацию об обнаружении вируса или подозрении на вирусное заражение и источнике, откуда был получен зараженный файл (владелец).

2.1.3.3. Возобновить работу только после удаления вирусной программы и нейтрализации последствий вирусного заражения.

2.1.4. Своевременно сообщать Администратору ИБ о выявленных фактах нарушений установленных настоящей инструкцией требований по обеспечению безопасности информации;

2.1.5. Обеспечивать сохранность выданных ему средств вычислительной техники, машинных носителей информации, персональных идентификаторов (token, смарт-карты, ibutton и т.п.);

2.1.6. Обеспечивать конфиденциальность информации, хранимой на выданных им машинных носителях информации;

2.1.7. Использовать выданные средства вычислительной техники и машинные носители информации исключительно в целях выполнения своих должностных обязанностей;

2.1.8. Контролировать действия в рабочем кабинете лиц, не имеющих право самостоятельного доступа в них.

2.2. Пользователь должен ознакомиться с положением о персональных данных, обрабатываемых в государственной информационной системе Камчатского края "Сетевой город" (сегмент 072).

2.3. Пользователь имеет право:

2.3.1. Вносить предложения по развитию и совершенствованию системы защиты информации при работе со средствами вычислительной техники;

2.3.2. Обращаться к Администратору ИБ за консультациями по вопросам обеспечения безопасности информации.

2.4. Пользователю категорически запрещается:

2.4.1. Вводить аутентификационную информацию в случае, если существует возможность наблюдения за вводом со стороны посетителей или посторонних лиц;

2.4.2. Записывать аутентификационную и идентификационную информацию (логин, пароль) на бумажных носителях и оставлять или хранить на рабочем месте.

2.4.3. Разглашать ставшую известной в ходе выполнения своих обязанностей информацию ограниченного доступа третьим лицам;

2.4.4. Копировать информацию ограниченного доступа на внешние носители непредусмотренные для обработки ПДн в случаях, не предусмотренных должностными обязанностями;

2.4.5. Использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

2.4.6. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

2.4.7. Несанкционированно открывать общий доступ к папкам на АРМ;

2.4.8. Умышленно использовать ошибки в программном обеспечении или в настройках АРМ (в том числе средств защиты), которые могут привести к возникновению кризисных ситуаций. Об обнаружении такого рода ошибок ставить в известность лицо, ответственное за организацию обработки персональных данных, либо Администратора ИБ;

2.4.9. Подключать к АРМ личные внешние носители и мобильные устройства;

2.4.10. Отключать (блокировать) средства защиты информации;

2.4.11. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ГИС;

2.4.12. Привлекать посторонних лиц для производства ремонта или настройки АРМ без согласования с Администратором ИБ;

2.4.13. Применять для обработки ПДн технологии беспроводного доступа и мобильные технические средства.

3. Ответственность.

3.1. Пользователь несет персональную ответственность за нарушение требований настоящей инструкции в соответствии действующим законодательством Российской Федерации.

заместитель директора по УВР
МБОУ «Средняя школа №7» _____ Гилязова О.С.
подпись