Приложение №1
к приказу от «25» 10 2024 г. № 214

ИНСТРУКЦИЯ
по эксплуатации информационных систем СПбГИПСР

1. Термины и определения

1.1. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

1.2. Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

1.3. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.4. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

1.5. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

1.6. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.7. Пользователь информационной системы – работник, осуществляющий обработку информации ограниченного доступа в информационной системе.

1.8. Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

1.9. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая инструкция определяет обязанности, права и ответственность ответственного за защиту информации в информационных системах (далее – ИС), администратора ИС и пользователей ИС СПбГИПСР (далее – Учреждение).

2.2. Требования настоящей инструкции являются обязательными для всех работников, осуществляющих обработку и защиту информации ограниченного доступа (далее – ИОД) в ИС.

2.3. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

3. Предоставление доступа к ресурсам

3.1. Пользователи получают возможность доступа к ресурсам ИС на основании соответствующего списка, утверждаемого ректором Учреждения, после ознакомления с локальными актами Учреждения по обработке и защите ИОД.

3.2. Пользователь обязан:

- знать и выполнять требования настоящей инструкции, а также действующих нормативных и руководящих документов регламентирующих порядок действий по защите ИОД;
- выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые требуются для выполнения его должностных обязанностей;
- работать в сетях общего доступа и (или) международного обмена, только при служебной необходимости;
- соблюдать установленные правила разграничения доступа к ИОД, обрабатываемой в ИС;
- при временном прекращении работы блокирует экран монитора при помощи механизмов средства защиты информации (далее – СЗИ) от несанкционированного доступа (далее – НСД) путем одновременного нажатия кнопок Windows и L на клавиатуре;
- знать и выполнять правила работы с СЗИ, установленными в ИС;
- немедленно ставить в известность ответственного за защиту информации в ИС и (или) администратора ИС, об обнаруженных инцидентах, в которые входят:
  - факты попыток и успешной реализации несанкционированного доступа в системы обработки ИОД, в помещения обработки ИОД и к хранилищам ИОД;
  - факты сбоя или некорректной работы систем обработки ИОД;
  - факты сбоя или некорректной работы СЗИ;
  - факты разглашения ИОД;
  - факты разглашения информации о методах и способах защиты и обработки ИОД.

3.3. Пользователю категорически запрещается:

- разглашать ИОД, ставшую известной ему по роду работы;
- производить действия в ИС в обход процедур идентификации и аутентификации в операционной системе;
- использовать неучтенные съемные машинные носители ИОД;
- вносить изменения в конфигурацию ИС;
- самостоятельно устанавливать или модифицировать программное и (или) аппаратное обеспечение ИС;
- подключать внешние устройства к ЭВМ: мобильные устройства, дисководы, модемы и т.д. (если это не требуется для выполнения трудовых обязанностей);
- отключать СЗИ;
- использовать компоненты программного и аппаратного обеспечения ИС в неслужебных (личных) целях;
- оставлять АРМ без присмотра, не активизировав СЗИ от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках СЗИ, которые могут привести к инцидентам информационной безопасности.

3.4. Пользователи ИС несут ответственность по действующему законодательству за разглашение сведений ограниченного доступа, ставших известными им по роду работы.

4. Организация работы со съемными машинными носителями информации

4.1. Организация работы со съемными машинными носителями ИОД, содержащие ИОД, осуществляется в соответствии с «Порядком по обращению со съемными машинными носителями информации ограниченного доступа в СПбГИПСР».

4.2. Пользователи обязаны знать и соблюдать установленные требования по учету и хранению съемных машинных носителей ИОД.

4.3. Съемные машинные носители ИОД должны быть зарегистрированы в «Журнале учета съемных машинных носителей информации ограниченного доступа».

4.4. Съемные машинные носители ИОД закрепляются за определенным лицом, несущим ответственность за сохранность и местонахождение данного съемного машинного носителя ИОД.

4.5. При необходимости передачи информации на съемном машинном носителе ИОД, лицо ответственное за хранение уведомляет ответственного за защиту информации в ИС о необходимости передачи информации с помощью съемного носителя ИОД, доставляет съемный машинный носитель ИОД по месту назначения, передает информацию с него и возвращает его на место хранения.

4.6. Хранение съемных машинных носителей ИОД осуществляется:

- для флеш-карт, смарт-карт, компакт дисков и др.) в защищенных сейфах;
- для машинных носителей, входящих в состав ИС, производится опечатывание корпуса АРМ.

4.7. Пользователям запрещается:

- записывать и хранить ИОД на неучтенных съемных машинных носителях ИОД;
- оставлять съемные машинные носители ИОД без присмотра, передавать их другим лицам и выносить за пределы контролируемой зоны, за исключением случаев, в которых разрешена передача съемных машинных носителей ИОД;
- хранить съемные машинные носители ИОД вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;
- хранить на учтенных съемных машинных носителях ИОД программы и данные, не относящиеся к рабочей информации.

5. Порядок организации парольной защиты

5.1. Пароли доступа к ИС выдаются администратором ИС.

5.2. Личные пароли доступа к АРМ из состава ИС создаются пользователем самостоятельно и должны соответствовать следующим требованиям:

- длина пароля не менее 6 символов;
- алфавит пароля не менее 60 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;
- блокировка программно-технического средства 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;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения и т.д.), а также общепринятые сокращения (anonymous, user, пользователь и т.п.).

5.3. Пользователю запрещается:

- Запрещается записывать пароли на бумажные носители, в файл, в электронную записную книжку и другие носители информации, в том числе на предметы. При возникновении сложностей с запоминанием, пароль может быть помещен в плотный конверт (исключающий просмотр «на просвет»). Конверт опечатывается (подписывается личной подписью работника) и хранится в металлическом хранилище (сейфе, отдельной ячейке сейфа или металлического шкафа). При отсутствии у работника своего хранилища конверт с паролем может храниться в сейфе руководителя подразделения. Способ запечатывания конверта должен исключать несанкционированный доступ к его содержимому без повреждения упаковки.
- Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.
- Оставлять АРМ включенным без личного присмотра, не заблокировав сеанс доступа в ИС.

5.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

5.5. Правила смены паролей:

- внеплановая смена личного пароля в случае возникновения компрометации пароля немедленно, утраты пароля;
- внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой;
- внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора ИС или ответственного за защиту информации в ИС;

5.6. Владельцы паролей обязаны своевременно сообщать администратору ИС об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

5.7. При отсутствии технической возможности самостоятельно произвести смену пароля пользователь сообщает о необходимости смены пароля администратору ИС.

6. Порядок организации антивирусной защиты

6.1. К использованию допускаются только лицензионные антивирусные средства, официально приобретенные у поставщиков.

6.2. Применяемые антивирусные средства должны иметь сертификат ФСТЭК России.

6.3. Средства антивирусной защиты должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в ИС.

6.4. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

6.5. Реализация антивирусной защиты должна предусматривать:

- проведение периодических проверок АРМ на наличие вредоносных компьютерных программ (вирусов);
- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

- оповещение в масштабе времени, близком к реальному об обнаружении вредоносных компьютерных программ (вирусов);
- определение и выполнение действий по реагированию на обнаружение в ИС объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

6.6. При резервном копировании информации, файлы, помещаемые в электронный архив, должны проходить антивирусный контроль с целью выявления вредоносных компьютерных программ.

6.7. Своевременное обновление баз данных средств антивирусной защиты является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

6.8. Обновление базы данных признаков вредоносных компьютерных программ (вирусов) производится один раз в сутки в автоматическом режиме.

6.9. Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);
- получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

6.10. Обязанности пользователей ИС:

- Пользователям категорически запрещается:
  - менять настройки средств антивирусной защиты или отключать их во время работы;
  - использовать средства антивирусной защиты, отличные от установленных средств;
  - без разрешения копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.
- Пользователи обязаны проверять съемные машинные носители (CD-диски, USB-флэш-накопители и т.д.) перед использованием на наличие вирусов.
- При получении подозрительного письма с вложением по электронной почте (письмо от неизвестного абонента, файл вложения с двойным расширением и т.п.) пользователям запрещается самостоятельно открывать файл вложения. Пользователь должен поставить в известность ответственного за защиту информации в ИС.
- Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения ответственного за защиту информации в ИС.
- В случае появления подозрений на наличие программных вирусов пользователи должны немедленно проинформировать об этом ответственного за защиту информации в ИС.
- В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений, поступивших в формационной системе, пользователь должен:
  - приостановить процесс приема-передачи информации;
  - сообщить ответственному за защиту информации в ИС о факте обнаружения программного вируса;
  - принять по согласованию с ответственным за защиту информации в ИС по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;
  - в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку;

– по факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

6.11. Все субъекты доступа: ответственный за защиту информации в ИС, администратор ИС, пользователи ИС несут ответственность за создание, распространение вредоносных программ, а также нарушений правил эксплуатации электронных вычислительных машин, системы электронных вычислительных машин или их сетей в соответствии с действующим законодательством РФ (ст.273, 274 гл.28 УК РФ).

7. Порядок организации обращения с программным обеспечением

7.1. Приобретением ПО занимается администратор ИС.

7.2. Установка и настройка любого программного обеспечения (далее – ПО), а также обновлений для ПО, осуществляется только администратором ИС.

7.3. Установка ПО производится только с носителей оригинальных лицензионных дистрибутивов, носителей эталонных копий ПО.

7.4. Установка и настройка ПО осуществляется в строгом соответствии с технической и эксплуатационной документацией на данное ПО.

7.5. Установке обновлений должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от вновь устанавливаемых обновлений.

7.6. В случае обнаружения негативного воздействия устанавливаемого обновления на штатное функционирование информационной инфраструктуры, данное обновление устанавливаться не должно.

7.7. Установке новых версий программного обеспечения или внесению изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного программного обеспечения.

7.8. Установка протестированных обновлений может быть произведена только администратором ИС на основании решения ответственного за защиту информации в ИС.

7.9. Установка новых версий программного обеспечения или внесение изменений и дополнений в действующее программного обеспечения может быть произведено только администратором ИС на основании решения ответственного за защиту информации в ИС.

8. Порядок организации резервирования и восстановления работоспособности программного обеспечения, баз данных и средств защиты информации

8.1. Резервирование программного обеспечения и баз данных выполняется администратором ИС.

8.2. Резервирование программных компонент СЗИ ИС выполняется ответственным за защиту информации в ИС.

8.3. Определяется 2 вида резервирования баз данных:

- полное резервирование – резервное копирование всех данных;
- неполное резервирование – резервное копирование части данных.

8.4. Целью неполного резервирования является сохранение изменений в ИС с момента полного резервирования баз данных.

8.5. Периодичность проведения работ по резервированию баз данных должна составлять не менее 1 раза в месяц для полного резервирования и 1 раза в неделю для неполного резервирования.

8.6. Для организации резервирования и восстановления работоспособности ПО должно быть обеспечено ведение двух копий программных средств и их периодическое обновление, и контроль работоспособности.

8.7. Для организации резервирования и восстановления работоспособности ПО, перед каждым обновлением ПО необходимо делать контрольную точку восстановления операционной системы.

8.8. При организации резервирования и восстановления работоспособности ПО сначала осуществляется резервное копирование баз данных, затем производится полная деинсталляция некорректно работающего ПО.

8.9. Администратор ИС, ответственный за защиту информации в ИС в пределах своих полномочий осуществляют:

- первоначальную настройку системы резервного копирования ПО (задание режимов резервного копирования, составление расписаний резервного копирования и т.д.);
- запуск в промышленную эксплуатацию системы резервного копирования.

8.10. При восстановлении работоспособности СЗИ следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты информации.

8.11. Ответственность за проведение мероприятий по восстановлению ПО возлагается на администратора ИС.

8.12. Ответственность за проведение мероприятий по восстановлению СЗИ возлагается на ответственного за защиту информации в ИС.

9. Ответственность

9.1. Все работники, осуществляющие обработку и защиту ИОД в ИС, обязаны ознакомиться с данной инструкцией под подпись.

9.2. работники несут персональную ответственность за выполнение требований настоящей инструкции.

10. Срок действия и порядок внесения изменений

10.1. Настоящая инструкция вступает в силу с момента ее утверждения и действует бессрочно.

10.2. Настоящая инструкция подлежит пересмотру не реже одного раза в три года.

10.3. Изменения и дополнения в настоящую инструкцию вносятся приказом ректора Учреждения.