УТВЕРЖДАЮ
Директор
МАОУ «Средняя общеобразовательная школа № 8 им. генерала-лейтенанта В.Г. Асапова г. Южно-Сахалинск»

_____
Н.А. Кораблева

«30» 04 2018 г.

ПОЛОЖЕНИЕ

о разграничении прав доступа к обрабатываемой информации в информационных системах МАОУ «Средняя общеобразовательная школа № 8 им. генерала-лейтенанта В.Г. Асапова г. Южно-Сахалинск»

Обозначения и сокращения
Учреждение – МАОУ «Средняя общеобразовательная школа № 8 им. генерала-лейтенанта В.Г. Асапова г. Южно-Сахалинск»
АРМ – автоматизированное рабочее место
ИС – информационная система
ОС – операционные системы
ПАК – программно-аппаратный комплекс
ПО – программное обеспечение
РПД – разграничение прав доступа
СЗИ - средства защиты информации
СКЗИ – средства криптографической защиты информации

Объект - это пассивный компонент системы, единица ресурса ИС (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.
Субъект - это активный компонент ИС (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.
Доступ к информации - ознакомление с информацией (чтение, копирование), ее модификация (корректировка), уничтожение (удаление) и т.п.
Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.
Несанкционированный доступ (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

1. Введение.

Положение о разграничении прав доступа к обрабатываемой информации в информационных системах Учреждения разработано в целях реализации требований нормативно правовых актов РФ в сфере защиты информации, политики информационной безопасности.
Основной задачей РПД является обеспечение доступности, конфиденциальности и целостности информации, обрабатываемой в ИС Учреждения.

2. Методы разграничений доступа.

Сотрудники Учреждения допускаются к обработке информации в ИС приказом руководителя.
Полномочия (права) доступа определяются администратором безопасности ИС, в соответствии с должностными обязанностями сотрудника, на основании матрицы доступа конкретной ИС.
Матрицу доступа (ПРД) для конкретной ИС утверждает руководитель Учреждения, после опытной эксплуатации ИС, на основании рекомендаций производителя и администратора ИС.
На основании матрицы доступа администратор ИС создает учётную запись для данного сотрудника и пароль.
Полномочия на создание, редактирование, удаление учетных записей делегировано администратору конкретной ИС. Контроль за управлением и соответствием РПД ведет администратор безопасности Учреждения.
В целях усиления контроля за ПРД в Учреждения применяются СЗИ и СКЗИ, имеющие сертификаты соответствия ФСТЭК и ФСБ РФ. Настройка СЗИ и СКЗИ производиться в соответствии с рекомендациями производителей.

3. Средства контроля и разграничения прав доступа.

В ИС применяются следующие технические средства разграничения доступа к ресурсам они рассматриваться как составная часть единой системы контроля доступа субъектов доступа к объектам доступа:

- на контролируемую территорию, в отдельные здания и помещения организации;
- к элементам ИС и элементам СЗИ (физический доступ);
- к информационным и программным ресурсам ИС.

4. Требования к размещению технических средств

При размещении технических средств ИС, предназначенных для обработки конфиденциальной информации выполнять следующие требования:

- должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства ИС, посторонних лиц, по роду своей деятельности, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на элементы ИС, технические средства, на которых эксплуатируется СЗИ и СКЗИ и защищаемую информацию;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

5. Требования к программному и аппаратному обеспечению

Технические средства ИС должны отвечать следующим требованиям:

- На технических средствах ИС должно использоваться только лицензионное ПО. Указанное ПО не должно содержать средств разработки или отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование ИС. В случае технологических потребностей организации, эксплуатирующей ИС, в использовании иного программного обеспечения, его применения должно быть санкционировано администратором безопасности. В любом случае ПО не должно содержать в себе возможностей, позволяющих:
  - модифицировать содержимое произвольных областей памяти;
  - модифицировать собственный код и код других подпрограмм;
  - модифицировать память, выделенную для других подпрограмм;
  - передавать управление в область собственных данных и данных других подпрограмм;
  - несанкционированное модифицировать файлы, содержащие исполняемые кода при их хранении на жестком диске;
  - использовать недокументированные фирмами-разработчиками функции.
- На АРМ одновременно может быть установлена только одна разрешенная ОС.
- На АРМ должны быть определены установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске.
- отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку.
- Средствами BIOS должна быть отключена возможность отключения пользователями PCI устройств при использовании ПАК защиты от НСД, устанавливаемых в PCI разъем;
- Вход в BIOS должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только администратору и быть отличным от пароля администратора для входа в ОС;
- Программные модули СКЗИ (прикладного ПО со встроенным СКЗИ) должны быть доступны только по чтению/запуску (в атрибутах файлов запрещена запись и модификация).

6. Защита информации от НСД

Для защиты от НСД необходимо принять следующие организационные меры:

- Предоставить права доступа к АРМ ИС только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию;

- Запретить осуществление несанкционированного администратором безопасности копирования носителей информации;
- Запретить использование носителей информации, не предусмотренных правилами пользования СКЗИ;
- Запретить пользователям оставлять без контроля АРМ, на которых обрабатывается информация. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки;
- Сдать носители информации в соответствии с порядком, установленным при увольнении или отстранении от исполнения обязанностей;
- Немедленно уведомлять администратора безопасности, либо руководителя подразделения о фактах утраты или недостачи носителей информации, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации;
- Запрещается разглашать содержимое носителей ключевой информации и передавать носители лицам к ним не допущенным;
- В случае обнаружения «посторонних» (незарегистрированных) программ или нарушения целостности программного обеспечения работа должна быть прекращена;
- Пользователь должен запускать только те приложения, которые разрешены администратором.

Администратор ИС должен сконфигурировать ОС, в среде которой планируется обрабатывать конфиденциальную информацию, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- Не использовать нестандартные, измененные или отладочные ОС;
- Исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
- Исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек;
- Правом установки и настройки ОС и СКЗИ должен обладать только администратор ИС;
- ОС должна быть настроена только для работы с СКЗИ. Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
- Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права;
- Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
  - Системный реестр;
  - Файлы и каталоги;
  - Временные файлы;
  - Журналы системы;
  - Файлы подкачки;
  - Кэшируемая информация (пароли и т.п.);
  - Отладочная информация.

Необходимо организовать затирание (по окончании сеанса работы) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

Необходимо регулярно устанавливать пакеты обновления безопасности ОС, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной

безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.

В случае подключения АРМ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи, данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети, применять СКЗИ прошедшие процедуру проверки соответствия.

Исключить одновременную работу в ОС нескольких пользователей.

7. Контроль за ПРД

Контроль состоянием ПРД в ИС должен проводиться на основании годового плана мероприятий по обеспечению защиты информации в ИС, утвержденного руководителем Учреждения.

Для проведения контроля могут привлекаться специалисты организаций, имеющих лицензию на техническую защиту конфиденциальной информации.

Результаты проверки доводятся до руководителя Учреждения

8. Ответственность.

Ответственность за разграничение прав доступа к обрабатываемой информации возлагается на администратора безопасности информации и системных администраторов Учреждения.

Лист ознакомления:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____