Утверждаю
Директор ТОГАПОУ
«Аграрно-промышленный колледж»
_____ Михайлюк И.Н.
11.03.2019

ИНСТРУКЦИЯ

администратора защиты информации автоматизированных систем
ТОГАПОУ «Аграрно-промышленный колледж»

1. Общие положения

1.1. Настоящая Инструкция администратора защиты информации автоматизированных систем ТОГАПОУ «Аграрно-промышленный колледж» (далее – Инструкция) разработана в соответствии с требованиями законодательства Российской Федерации в области защиты конфиденциальной информации, а также руководящими документами ФСТЭК России и ФСБ России.

1.2. Инструкция является руководящим документом для администратора защиты информации автоматизированных систем ТОГАПОУ «Аграрно-промышленный колледж» (далее – администратор). Требования настоящей инструкции должны выполняться во всех режимах функционирования автоматизированных систем (далее АС).

1.3. Нарушение установленных требований и норм по защите информации по степени важности делятся на три категории:

– первая – невыполнение требований и норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам или несанкционированного доступа к ней (далее НСД);

– вторая – невыполнение требований и норм по защите информации, в результате чего создаются предпосылки к ее утечке по техническим каналам или НСД;

– третья – невыполнение других требований по защите информации.

1.4. При выявлении нарушения первой категории администратор обязан немедленно прекратить работы в АС и подать служебную записку руководству, в которой изложить факт нарушения, предпринятые и (или) рекомендуемые им действия.

1.5. При выявлении нарушений второй и третьей категорий администратор обязан подать служебную записку руководству, в которой изложить факт нарушения, предпринятые и (или) рекомендуемые им действия.

1.6. В своей повседневной деятельности администратор руководствуется документами, регламентирующими защиту конфиденциальной информации от утечки по техническим каналам и НСД и эксплуатационной документацией на установленные на объекте информатизации системы защиты (далее СЗИ) и от утечки информации по техническим каналам.

2. Общие обязанности администратора

Администратор защиты информации должен знать:

– законодательные и нормативные правовые акты, методические и нормативные материалы по вопросам, связанным с обеспечением информационной безопасности;

– структуру защищаемой системы, категории защищаемой информации, категории пользователей, работающих в системе и их права по доступу к ресурсам АС;

– порядок использования, обработки и хранения конфиденциальной информации в АС;

– методы и средства контроля защищаемой информации, способы выявления каналов утечки информации, способы организации противодействия угрозам информационной безопасности;

– принципы функционирования, методику обслуживания и устранения неисправностей программно-технических средств системы защиты информации;

– принципы работы и форматы файлов регистрации (журналирования) ОС, СУБД и приложений;

– основы сетевого администрирования;

– основы администрирования, используемых в СЗИ операционных систем, средств защиты информации и программного обеспечения;

– правила и нормы охраны труда.

Администратор защиты информации обязан:

– проводить совещательные мероприятия и инструктажи, направленные на повышение уровня квалификации работников в области информационной безопасности;

– поддерживать в актуальном состоянии таблицу разграничения доступа (матрицу доступа) к защищаемым ресурсам АС и своевременно её корректировать;

– не допускать использования, хранения и размножения в АС программных продуктов и носителей информации, непосредственно не связанных со служебной деятельностью на данном рабочем месте;

– не допускать к работе в АС посторонних лиц;

– участвовать в планировании эксплуатации АС при изменении условий её эксплуатации, контролируя выполнение требований Аттестата соответствия объекта информатизации;

– участвовать в разработке организационных мероприятий по обеспечению защиты информации при обработке конфиденциальной информации;

– поддерживать в актуальном состоянии и осуществлять хранение документации на объект;

– знать уровень конфиденциальности обрабатываемой информации, следить за тем, чтобы обработка информации производилась только с использованием учтенных съемных и несъемных носителей информации, причем уровень конфиденциальности последних должен быть не ниже уровня конфиденциальности обрабатываемой информации;

– поддерживать в актуальном состоянии журналы АС;

– вести оперативный анализ журналов регистрации событий, системных журналов и журналов безопасности, создавать архивные копии журналов и обеспечивать надёжное хранение этих копий. При обнаружении предпосылок и фактов НСД к защищаемым ресурсам АС принимать необходимые меры;

– осуществлять установку, настройку и контроль функционирования средств защиты информации в случае нарушения возникновения нештатных ситуаций и нарушения установленного технологического процесса обработки информации;

– контролировать целостность (неизменность), сохранность средств защиты информации, используемых в АС, а при обнаружении фактов изменения контролируемых параметров немедленно принимать меры по приведению контролируемых параметров в исходное состояние и докладывать руководству;

– обеспечивать контроль работы средств защиты информации, применяемых на объекте информатизации, а также контроль выполнения, установленного распорядительными документами комплекса организационных мероприятий по защите информации;

– осуществлять оперативные действия по конфигурированию СЗИ и поддержке ее компонентов в работоспособном состоянии, включая:

– актуализацию перечня защищаемой информации;

– поддержание в актуальном состоянии перечня учётных записей пользователей и назначенных им прав доступа к ресурсам;

– контролировать защищенность аппаратных средств АС;

– проводить периодическое тестирование средств защиты информации, осуществлять контроль их эксплуатации;

– осуществлять контроль требований защиты информации при проведении технического обслуживания и ремонта аппаратных средств АС;

– осуществлять постоянный контроль за соблюдением пользователями порядка антивирусной защиты, а также за отсутствием на АРМ пользователей, не учтённых в технических паспортах на АС программных средств, средств отладки ПО и непредусмотренных организационной документацией учётных записей пользователей.

Администратор защиты информации имеет право:

– запрашивать и получать от руководства и сотрудников информацию и материалы, необходимые для надлежащего исполнения своих должностных прав и обязанностей;

– в пределах своей компетенции сообщать непосредственному руководителю обо всех выявленных в процессе осуществления должностных обязанностей недостатках в работе АС и вносить предложения по их устранению;

– осуществлять взаимодействие с руководителями структурных подразделений колледжа по вопросам защиты информации;

– знакомиться с проектами решений руководства колледжа, касающимися его деятельности;

– подписывать и визировать документы в пределах своей компетенции;

– получать доступ к аппаратным средствам АС и в защищаемые помещения, в которых они расположены;

– получать доступ к функциям администрирования средств защиты информации, применяемым в АС;

– получать полный доступ к журналам регистрации событий АС.

Администратор защиты информации несет ответственность:

– за невыполнение и/или несвоевременное, некачественное, халатное выполнение своих должностных обязанностей;

– за несоблюдение действующих инструкций, приказов и распоряжений;

– за разглашение защищаемой информации, ставшей ему известной в ходе исполнения своих должностных обязанностей;

– за качество проводимых им работ по контролю действий пользователей при работе в АС, состояние и поддержание установленного уровня защиты;

– за нарушение правил внутреннего трудового распорядка, трудовой дисциплины, правил техники безопасности и противопожарной безопасности.

3. Обязанности администратора по предотвращению утечки информации по техническим каналам

3.1. Администратор обязан контролировать выполнение требований Аттестата соответствия объекта информатизации, соответствие состава и расположения ОТСС и ВТСС техническому паспорту объекта информатизации и не допускать их нарушения.

3.2. Администратор обязан не допускать:

– внесение несанкционированных изменений в состав и размещение ОТСС и ВТСС, а также в схемы их соединений;

– изменение и состава и размещения средств защиты информации, если они установлены в помещениях объекта;

– внесение несанкционированных изменений в системы электроснабжения, заземления и других проводных коммуникаций объекта;

– обработку конфиденциальной информации при открытых (снятых) кожухах (крышках) основных технических средств и систем, а также при выключенных средствах защиты информации.

3.3. Администратор обязан периодически осуществлять контроль работоспособности системы защиты согласно эксплуатационной документации на систему.

4. Обязанности администратора по предотвращению несанкционированного доступа к обрабатываемой информации

4.1. При настройке СЗИ в АС пользователя администратор обязан установить минимальную длину пароля пользователя не менее 6 буквенно-цифровых символов.

4.2. Администратор обязан пресекать действия пользователей, которые могут привести к компрометации паролей (запись паролей пользователей в блокноты, тетради и т.д., произнесение паролей вслух в присутствии третьих лиц).

4.3. Администратор устанавливает правила разграничения доступа пользователей к защищаемым ресурсам АС средствами СЗИ в строгом соответствии с разработанной и утвержденной Матрицей доступа. Изменения в правила разграничения доступа допускается вносить только после внесения их в Матрицу доступа. При этом подпись лица, утвердившего ее, обязательна.

4.4. Для проведения анализа устойчивости системы защиты, определения скрытых каналов утечки информации администратор осуществляет сбор, хранение и анализ учетной информации СЗИ.

4.5. Администратор обязан регулярно (не менее 1 раза в месяц) анализировать содержимое системных журналов СЗИ.

4.6. При необходимости проведения обслуживания или ремонта средств вычислительной техники администратор организовывает согласование с организацией, проводившей работы.

4.7. Для обеспечения неизменности программного обеспечения СЗИ администратор обязан использовать средства контроля целостности СЗИ в соответствии с эксплуатационной документацией СЗИ.

5. Обязанности администратора по предотвращению утечки информации при межсетевом взаимодействии.

Задачами Администратора по поддержанию защищённого межсетевого взаимодействия являются:

– конфигурирование сертифицированных средств межсетевого экранирования и поддержание актуальных параметров безопасности межсетевого взаимодействия;

– анализ журналов регистрации и учета событий безопасности межсетевого взаимодействия;

– контроль целостности программной и информационной части сертифицированных средств межсетевого экранирования;

– осуществление процедур восстановления межсетевого взаимодействия.

6. Заключение

6.1. Настоящая Инструкция доводится до администратора защиты информации автоматизированной системы под подпись.

6.2. Настоящая Инструкция вступает в силу с момента её утверждения директором ТОГАПОУ «Аграрно-промышленный колледж».