МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ САМАРСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
«ТОЛЬЯТТИНСКИЙ ХИМИКО-ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

УТВЕРЖДАЮ

и. о. директора ГБПОУ «Тольяттинский химико-технологический техникум»

_____ Т. А. Михайленко

Приказ от «23» января 2019 г. № 6/1-од

Инструкция

ответственного за организацию обработки персональных данных в информационных системах в ГБПОУ «Тольяттинский химико-технологический техникум»

СОГЛАСОВАНО

Советом Учреждения
протокол от 22.01.2019 г. № 1

1. Общие положения

1.1. Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн) в ГБПОУ «Тольяттинский химико-технологический техникум» (далее – Учреждение).

1.2. Инструкция разработана на основании действующих законных, подзаконных нормативных актов, нормативно-методических и руководящих документов в области защиты персональных данных.

1.3. Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

1.4. Администратор информационной безопасности назначается приказом директора Учреждения.

1.5. Администратор информационной безопасности в своей работе должен руководствоваться настоящей Инструкцией, утвержденными документами ГБПОУ «Тольяттинский химико-технологический техникум» (далее - Учреждение), регламентирующими порядок обеспечения безопасности персональных данных, законными, подзаконными, руководящими документами по защите персональных данных, а также документами, поступившими из вышестоящих и контролирующих органов.

1.6. На должность администратора информационной безопасности назначаются сотрудники Учреждения, которые имеют широкие полномочия и способны организовать работы, необходимые для реализации требований законодательства, и имеющий достаточный опыт работы по основной деятельности Учреждения. На период отпуска или в случае временной нетрудоспособности ответственного за организацию обработки персональных данных назначается должностное лицо, временно исполняющие его обязанности.

1.7. Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

2. Обязанности администратора информационной безопасности

2.1. Администратор информационной безопасности обязан:

– знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;

– знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

– уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

– еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

– обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;

– участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

– обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

– обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

– обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

– обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

– обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

– обязан проводить мероприятия по организации антивирусной защиты;

– осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;

– обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

– обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

– установить причины, по которым стал возможным НСД;

– установить последствия, к которым привел НСД;

– зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

– провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;

– провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3. Права администратора информационной безопасности.

3.1. Администратор информационной безопасности имеет право:

– требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

– инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

– обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

– Приостанавливать работу пользователей в случае нарушения предъявляемых требований к защите персональных данных.

– способы и методы совершенствования системы защиты информации.

4. Ответственность администратора информационной безопасности

4.1. На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

4.2. Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение

ЖУРНАЛ
учета машинных носителей персональных данных (стационарные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета машинных носителей персональных данных (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание