Организация и проведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
ГБПОУ «Дзержинский индустриально-коммерческий техникум»

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных
ГБПОУ «Дзержинский индустриально-коммерческий техникум»

При организации и осуществлении защиты персональных данных (ПДн) необходимо руководствоваться требованиями нормативных и методических документов по защите информации в автоматизированных системах (информационных системах персональных данных – ИСПДн), учитывая при этом, что ПДн, в соответствии с Федеральным Законом от 27 июля 2006 года № 152 – ФЗ «О персональных данных» и Указом Президента РФ № 188 от 06.03.97 г., отнесены к конфиденциальной информации.

Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

При проведении мероприятий по защите ПДн учитывается, что информационные ресурсы подвержены потенциальным внешним и внутренним угрозам, ведущим к потерям конфиденциальности, доступности и целостности информационных ресурсов.

Источники угрозы:

- люди (недобросовестные внешние и внутренние пользователи информационных ресурсов);
- аварии (ошибки пользователя, ошибки администратора);
- отказ аппаратного обеспечения (ошибки программного обеспечения, отказы индустриального оборудования);
- природные факторы (стихийные бедствия, астрофизические явления, биологические явления).

Угрозы увеличивают риски безопасности, представляющие собой:

- неавторизированный доступ в сеть;
- неавторизированное раскрытие информации;
- неавторизированную модификацию данных или программного обеспечения;
- разрушение функций сети (недоступность данных и сервисов).

Наличие рисков безопасности требуют введения мер безопасности. Меры безопасности должны гарантировать:

- конфиденциальность;
- целостность;
- доступность информации;
- своевременное получение отчетности;
- физическую безопасность информации;
- контроль доступа к информации.

Информационная безопасность предусматривает:

- процедурную (административную и организационную безопасность);
- безопасность персонала;
- физическую безопасность;
- безопасность системы;
- безопасность коммуникаций.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Мероприятия по обеспечению безопасности ПДн проводятся в зависимости от типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, с учетом возможного возникновения угроз безопасности жизненно мероприятия, направленные на:

- предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, организациям, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- оперативного резервирования информации в ИСПДн;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- постоянный контроль за обеспечением уровня защищенности ПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (СЗПДн).

Структура, состав и основные функции СЗПДн определяются в зависимости от типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, используемых в Училище.

СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

В интересах технического обеспечения безопасности ПДн при их обработке в ИСПДн, в зависимости от класса информационной системы должны быть проведены мероприятия по защите от НСД к ПДн при их обработке в ИСПДн.

В состав мероприятий по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий входят следующие мероприятия:

- защита от НСД при однопользовательском режиме обработки ПДн;
- защита от НСД при многопользовательском режиме обработки ПДн и равных правах доступа к ним субъектов доступа;
- защита от НСД при многопользовательском режиме обработки ПДн и разных правах доступа;
- защита информации при межсетевом взаимодействии ИСПДн;
- антивирусная защита.

Мероприятия по защите ПДн реализуются в рамках подсистем: управления доступом, регистрации и учета, обеспечения целостности, криптографической защиты, антивирусной защиты.

Меры безопасности ПДн должны гарантировать:

- конфиденциальность;
- целостность;

- доступность информации.

Мероприятия по обеспечению безопасности предусматривают:

- управление доступом;
- регистрацию и учет;
- обеспечение целостности;
- контроль отсутствия недекларированных возможностей;
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия;
- анализ защищенности.

Подсистемы управления доступом и регистрации и учета должны реализовываться на базе программных средств блокирования несанкционированных действий, сигнализации и регистрации. Это специальные, не входящие в ядро какой-либо операционной системы программные и программно-аппаратные средства защиты самих операционных систем, электронных баз данных и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения опасных действий пользователя или нарушителя.

Средства диагностики должны осуществлять тестирование файловой системы и баз данных, постоянный сбор информации о функционировании элементов подсистемы обеспечения безопасности информации.

Средства уничтожения предназначены для уничтожения остаточных данных и должны предусматривать аварийное уничтожение данных в случае угрозы несанкционированного доступа (НСД), которая не может быть блокирована системой.

Средства сигнализации предназначены для предупреждения операторов (пользователей) при их обращении к защищаемым данным и для предупреждения администратора при обнаружении факта НСД, искажении программных средств защиты, выходе или выводе из строя аппаратных средств защиты и о других фактах нарушения штатного режима функционирования.

Подсистема обеспечения целостности должна быть реализована операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

Подсистема контроля отсутствия недекларированных возможностей должна реализовываться на базе систем управления базами данных, средств защиты информации, антивирусных средств защиты информации.

Для осуществления разграничения доступа к информационным ресурсам при межсетевом взаимодействии должно применяться межсетевое экранирование, которое реализуется программными и/или программно-аппаратными межсетевыми экранами (МЭ). Межсетевой экран должен устанавливаться

между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран должен входить в состав защищаемой сети. При его настройке отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Подсистема анализа защищенности должна реализовываться на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности информации.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе назначается структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных в информационных системах персональных данных.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, должны допускаться к соответствующим персональным данным на основании утвержденных Перечней должностных лиц, допущенных к работе с персональными данными.

Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в утвержденных Перечнях должностных лиц, а также факты предоставления персональных данных по этим запросам должны регистрироваться автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) Училища или уполномоченными лицами.

При обнаружении нарушений порядка предоставления персональных данных Техникума уполномоченные лица должны незамедлительно приостановить предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

При хранении материальных носителей информации с персональными данными (или другой конфиденциальной информацией) должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются отдельно.