Приложение № 1

к Приказу от «25» октября 2018 № 2211

**Концепция информационной безопасности**

**в ИСПДн «УПЭИОС» УлГТУ**

Введение

Настоящая Концепция информационной безопасности ИСПДн «УПЭИОС» УлГТУ является документом, в котором определена система взглядов на обеспечение информационной безопасности.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн). Концепция определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации.

Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности, а также нормативных и методических документов, обеспечивающих ее реализацию.

Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн). Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

СЗПДн представляет собой совокупность организационных и тех­нических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, рас­пространения ПДн, а также иных неправомерных действий с ними.

Безопасность персональных данных 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 иных несанкционированных действий.

Структура, состав и основные функции СЗПДн определяются исходя из необходимого уровня защищенности ИСПДн. СЗПДн включает организационные меры и технические средства защиты.

Эти меры призваны обеспечить:

* **конфиденциальность** информации (защита от несанкционированного ознакомления);
* **целостность** информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
* **доступность** информации (возможность за приемлемое время получить требуемую информационную услугу).

Организационные меры предусматривают создание следующих организационно-распорядительных документов:

* Приказов, [план](Приложение%2012%20План%20мероприятий%20по%20обеспечению%20защиты%20ПДн.doc)ов и других необходимых документов для обеспечения  [мероприятий по защите ПДн](Приложение%2014%20План%20внутренних%20проверок.doc);
* [Должностной инструкции администраторов ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн](Приложение%2017%20Инструкция%20администратора%20ИСПДн.doc);
* [Должностной инструкции администраторов информационной безопасности ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн](Приложение%2017%20Инструкция%20администратора%20ИСПДн.doc);
* [Должностной инструкции пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн](Приложение%2018%20Инструкция%20пользователя%20ИСПДн.doc);
* [Инструкции на случай возникновения внештатной ситуации](Приложение%2020%20Инструкция%20пользователя%20по%20обеспечению%20безопасности%20обработки%20персональных%20данных,%20при%20возникновении%20внештатных%20ситуаций.doc);
* Рекомендации по использованию программных и аппаратных средств защиты информации.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам определения необходимого "Уровня защищенности".

Задачи СЗПДн

Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

* защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования ИСПДн и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);
* разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей);
* регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;
* контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
* защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;
* своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;
* создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

Объекты защиты

В УлГТУ производится обработка персональных данных в информационной системе обеспечения учебного процесса с элементами электронной информационной общеобразовательной среды на базе «1С -Университет» (ИСПДн «УПЭИОС» УлГТУ).

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты.

Классификация пользователей ИСПДн

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Пользователи ИСПДн делятся на четыре основные категории:

Администраторы ИСПДн. Сотрудники, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уровнем доступа:

* + обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
  + обладает полной информацией о технических средствах и конфигурации ИСПДн;
  + имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
  + обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Администраторы ИБ ИСПДн. Сотрудники, которые занимаются настройкой, внедрением и сопровождением системы защиты ПДн. Администратор ИБ ИСПДн обладает следующим уровнем доступа:

* + обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
  + обладает полной информацией о технических средствах и конфигурации ИСПДн;
  + имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
  + обладает правами конфигурирования и административной настройки технических средств защиты информации в ИСПДн.

Программист-разработчик ИСПДн. Сотрудники занимаются разработкой программного обеспечения. Разработчик ИСПДн обладает следующим уровнем доступа:

* + обладает информацией об алгоритмах и программах обработки информации в ИСПДн;
  + обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
  + может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

Оператор (пользователь) ИСПДн. Сотрудники подразделений, участвующих в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

* + обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к части ПДн;
  + располагает конфиденциальными данными, к которым имеет доступ.

Модель нарушителя безопасности

Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

* внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
* внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Для ИСПДн «УПЭИОС» УлГТУ актуальны внутренние нарушители угроз безопасности персональных данных.

Модель угроз безопасности

Для ИСПДн УлГТУ актуальны следующие категории угроз безопасности персональных данных:

* + Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.
  + Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.
  + Угрозы преднамеренных действий внутренних нарушителей.

Меры безопасности

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

* организационные (административные);
* технические (аппаратные и программные).

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

В организационные меры включаются:

* регламент доступа в серверные помещения ИСПДн;
* порядок допуска сотрудников к использованию ресурсов ИСПДн;
* регламент процессов ведения баз данных и осуществления модификации информационных ресурсов;
* регламент процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;
* инструкции администраторов ИСПДн;
* инструкции пользователей ИСПДн;

Технические (аппаратно-программные) меры защиты основаны на использовании специальных программных средств, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, и т.д.).

В состав системы защиты должны быть включены следующие средства:

* средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
* средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн;
* средства обеспечения и контроля целостности программных и информационных ресурсов;
* средства оперативного контроля и регистрации событий безопасности

Контроль эффективности системы защиты ИСПДн

Контроль эффективности СЗПДн должен осуществляться на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Приложение № 2