I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности (далее – Политика) федерального государственного бюджетного образовательного учреждения высшего образования «Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского» (далее – ФГБОУ ВО «ДОННУЭТ», Университет) является локальным нормативным актом и определяет цель и задачи защиты информации, основные принципы и способы достижения требуемого уровня информационной безопасности в Университете.

1.2. Положения и требования данного документа распространяются на все структурные подразделения Университета, включая филиалы, и являются обязательными для выполнения всеми работниками ФГБОУ ВО «ДОННУЭТ».

1.3. Законодательной основой настоящей Политики являются:

– Конституция Российской Федерации;

– Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

– Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне»;

– Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;

– Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Постановление правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя

органа (организации), ответственного за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»;

– Инструкция о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки Российской Федерации, утвержденная Приказом Министерства образования и науки Российской Федерации от 30.12.2010 № 2233.

1.4. Политика является методологической основой для:

– создания единой системы управления информационной безопасностью Университета;

– принятия управленческих решений, разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

– координации деятельности структурных подразделений Университета при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации;

– разработки предложений по совершенствованию правового, нормативного, организационного и технического обеспечения безопасности информации.

II. ОБЛАСТЬ ДЕЙСТВИЯ

2.1. Настоящая Политика распространяется и влияет на все виды деятельности ФГБОУ ВО «ДОННУЭТ», на всю обрабатываемую в Университете информацию, на любые информационные системы и ресурсы, средства обработки информации, а также на всех работников и обучающихся ФГБОУ ВО «ДОННУЭТ», а также заинтересованных лиц (включая контрагентов, лиц, работающих по договорам гражданско-правового характера и других лиц).

2.2. *Обработка информации* – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, извлечение, использование, передачу (распространение, предоставление), блокирование, удаление, уничтожение информации в любой форме.

2.3. Настоящая политика распространяется и влияет на все формы

представления информации – электронную, на бумажных носителях, устную, визуальную, электромагнитную и другие формы.

III. ЦЕЛЬ ПОЛИТИКИ

3.1. Политика направлена на защиту информационных ресурсов, информационной инфраструктуры и процессов обработки информации Университета от возможного нанесения им материального, физического или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи ее по каналам связи, а также минимизацию подобных рисков.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

– *доступности информации* – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

– *целостности информации* – состояние, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

– *конфиденциальности* – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

3.2. Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается применением соответствующих мер информационной безопасности.

3.3. Для достижения цели политики и обеспечения указанных свойств должны выполняться следующие задачи:

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы;

– создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями внутренних и внешних нарушителей, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

– разграничение доступа пользователей к информационным, аппаратным,

программным и иным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей);

– обеспечение идентификации и аутентификации пользователей информационных ресурсов;

– категорирование информации с точки зрения нормативных правовых требований, ценности, критичности и чувствительности к неавторизованному раскрытию или модификации;

– защита от несанкционированной модификации используемых в информационной системе программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

– защита конфиденциальной информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

IV. СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ. ОСНОВНЫЕ ФУНКЦИИ

4.1. Система управления информационной безопасностью является частью общей системы управления Университетом и предназначена для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности.

4.2. Организация работы и эффективное функционирование системы управления информационной безопасностью в Университете, возлагается на управление цифровой трансформации и информационных технологий (далее – УЦТИТ).

Управление цифровой трансформации и информационных технологий, для выполнения конкретных задач в области информационной безопасности вправе привлекать иные структурные подразделения Университета, сторонние организации, имеющие соответствующие лицензии на данный вид деятельности, а также создавать рабочие группы и комиссии.

4.3. Основные функции:

– организация системы защиты информации, контроль соблюдения требований законодательства Российской Федерации в сфере информационной безопасности;

– создание единой концепции информационной безопасности, определение мероприятий, направленных на ее реализацию;

– планирование и реализация задач, способствующих повышению уровня информационной безопасности;

– организация и проведение мероприятий по информационной

безопасности;

– реализация, развитие и поддержка системы антивирусной защиты;

– выявление технических каналов утечки информации, в том числе за счет несанкционированного доступа к информации, а также ее разрушения (уничтожения) или искажения, разработка соответствующих мер по защите информации;

– обеспечение безопасности информационной инфраструктуры;

– обеспечение сохранности информационных ресурсов, соблюдения правильности выполнения процессов обработки информации и защите информационной инфраструктуры;

– контроль за соблюдением требований информационной безопасности подчиненным и работниками;

– соблюдение порядка обращения с конфиденциальной информацией в т.ч. документами, носителями ключевой информации и другой защищаемой информации;

– выполнение требований настоящей Политики и других документов по информационной безопасности.

V. ОБЪЕКТЫ ЗАЩИТЫ

5.1. Объектами, подлежащими защите в соответствии с настоящей Политикой, являются:

– *информационные ресурсы*, содержащие конфиденциальную информацию (служебная информация ограниченного распространения, информация, составляющая коммерческую и государственную тайну, персональные данные (работников, обучающихся, аспирантов, докторантов, абитуриентов, лиц, выполняющих работы по договорам гражданско-правового характера, партнеров), открытая (общедоступная) информация, необходимая для осуществления деятельности университета и иная чувствительная информация;

– *процессы обработки информации в информационных системах* университета, информационные технологии (регламенты и процедуры сбора, обработки, хранения, выдачи и передачи информации);

– *информационная инфраструктура*, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной среды.

VI. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Меры обеспечения информационной безопасности подразделяются на: правовые; организационные; технические (аппаратные, программные, криптографические).

6.2. К *правовым мерам* относятся выполнение норм действующего законодательства в области защиты информации.

Правовые меры устанавливают правила использования информации и определяют ответственность за нарушение этих правил.

6.3. *Организационные меры* – это меры организационного характера, регламентирующие процессы функционирования информационных систем, деятельность обслуживающего персонала, а также порядок действия пользователей таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

6.4. *Технические меры* заключаются в обеспечении безопасности объектов защиты путем применения технических, программных, аппаратных, программно-аппаратных и криптографических средств защиты информации.

VII. ЛОКАЛЬНЫЕ НОРМАТИВНЫЕ АКТЫ УНИВЕРСИТЕТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Реализация положений настоящей Политики в ФГБОУ ВО «ДОННУЭТ» предусматривает принятие отдельных локальных нормативных актов: регламентов, требований, положений, инструкций и иных документов.

Принятие таких документов направлено на разъяснение и конкретизацию отдельных положений Политики, а также обеспечение безопасности информации, подлежащей защите в соответствии с законодательством Российской Федерации, информационной инфраструктуры, процессов обработки информации, порядка обращения с конфиденциальной информацией, безопасностью персональных данных и обеспечения физической и инженерно-технической безопасности объектов Университета.

VIII. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Система защиты персональных данных (СЗПДн), строится на основании:

– результатов проведения внутренней проверки;

– перечня персональных данных, подлежащих защите;

– акта классификации информационной системы персональных данных;

– Модели угроз безопасности персональных данных;

– Положения о разграничении прав доступа к обрабатываемым персональным данным;

– документов ФСТЭК и ФСБ России.

8.2. На основании этих документов определяется необходимый уровень защищенности персональных данных (далее – ПДн) в информационной системе персональных данных (далее – ИСПДн). На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз, и Акта о результатах проведения проверки, формируется заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

8.3. Для ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

– автоматизированное рабочее место (далее – АРМ) пользователей;

– сервер приложений;

– система управления базами данных (далее – СУБД);

– граница локальных вычислительных сетей (далее – ЛВС);

– каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

8.4. В зависимости от установленного уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

– антивирусные средства для рабочих станций пользователей и серверов;

– средства межсетевого экранирования;

– средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

8.5. Так же в список включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

– управление и разграничение доступа пользователей;

– регистрацию и учет действий с информацией;

– обеспечивать целостность данных;

– производить обнаружений вторжений.

8.6. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены лицом, ответственным за обеспечение защиты ПДн.

IX. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДН

9.1. СЗПДн включает в себя следующие подсистемы:

– управления доступом, регистрации и учета;

– обеспечения целостности и доступности;

– антивирусной защиты;

– межсетевого экранирования;

– анализа защищенности;

– обнаружения вторжений;

– криптографической защиты.

9.2. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

– идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;

– идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

– идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

– регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.

– регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

9.3. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств, а также средств защиты, при случайной или намеренной модификации.

9.4. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей.

Средства антивирусной защиты предназначены для реализации следующих функций:

– резидентный антивирусный мониторинг;

– антивирусное сканирование;

– скрипт-блокирование;

– централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

– автоматизированное обновление антивирусных баз;

– ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

– автоматический запуск сразу после загрузки операционной системы.

9.5. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

– фильтрации открытого и зашифрованного (закрытого) IP-трафика по определенным параметрам;

– фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

– идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

– регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы;

– контроля целостности своей программной и информационной части;

– фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

– регистрации и учета запрашиваемых сервисов прикладного уровня;

– блокирования доступа не идентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

– контроля за сетевой активностью приложений и обнаружения сетевых атак.

9.6. Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

9.7. Подсистема обнаружения вторжений должна обеспечивать выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена.

9.8. Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации ИСПДн при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

X. ПОЛЬЗОВАТЕЛИ ИСПДН

10.1. В ИСПДн выделяются следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратор безопасности;
- Администратор сети;
- Пользователь АРМ (привилегированный, обычный, с ограниченными правами).

Данные о группах пользователях, уровне их доступа и информированности отражен в Положение о разграничении прав доступа к обрабатываемым персональным данным в информационной системе персональных данных ФГБОУ ВО «ДОННУЭТ».

XI. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДн

11.1. Все сотрудники ФГБОУ ВО «ДОННУЭТ», являющиеся Пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

11.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

11.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

11.4. Пользователи, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

11.5. Пользователи должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

11.6. Пользователи должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать

требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

11.7. Пользователям запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

11.8. Пользователям запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.

11.9. При работе с ПДн Пользователи обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

11.10. При завершении работы с ПДн Пользователи обязаны защитить АРМ или терминалы с помощью блокировки или эквивалентного средства контроля, например, доступом по паролю.

11.11. Пользователи должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

11.12. Пользователи обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

XII. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ

12.1. Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации электронных вычислительных машин (далее – ЭВМ) и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (ст. 272 - 274 Уголовного кодекса Российской Федерации).

12.2. Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

12.3. При нарушениях сотрудниками-пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

XIII. КОНТРОЛЬ И ОТВЕТСТВЕННОСТЬ

13.1. Общий контроль за соблюдением требований, предписанных настоящей Политикой, возлагается на УЦТИТ.

13.2. Контроль и профилактика нарушений информационной безопасности и защиты информации осуществляется на плановой и внеплановой основах.

13.3. Контроль (оценка) эффективности принятых технических мер по защите информации проводится УЦТИТ самостоятельно или привлекаемыми для этой цели организациями, имеющими соответствующие лицензии на данный вид деятельности.

13.4. Нарушение положений настоящей Политики может повлечь за собой дисциплинарную, административную, гражданско-правовую, уголовную или иную ответственность в соответствии с законодательством Российской Федерации.

СОГЛАСОВАНО:

Проректор по комплексной безопасности К.А. Еропутов

Начальник отдела по юридическому и правовому обеспечению В.В. Калайда