	Частное образовательное учреждение высшего образования «Таганрогский институт управления и экономики»
	Положение о безопасности в информационных системах ТИУиЭ

«УТВЕРЖДАЮ»
Ректор ТИУиЭ

_____ /С.Ю. Аваков/
«__9__» ____01____ 2020 г.

ПОЛОЖЕНИЕ О БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ТИУиЭ

Введено приказом ректора от 9.01.2020 г. № 2

Таганрог-2020

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о безопасности в информационных системах (далее – Положение) Таганрогского института управления и экономики (ТИУиЭ) (далее – Институт) определяет единые нормы, правила и требования к системе управления информационной безопасностью (ИБ) Института.

1.2. Система обеспечения ИБ представляет собой совокупность нормативно-правовых, организационных, технических мер по обеспечению защищенности интересов Института в информационной сфере и субъектов информационных отношений.

1.3. Основные цели внедрения системы управления ИБ Института:

- защита конфиденциальности информационных ресурсов;
- обеспечение непрерывного авторизованного доступа к информационным ресурсам Института для поддержки основной деятельности;
- защита целостности информации для обеспечения требуемого качества работ и эффективности процесса принятий решений;
- установление ответственности за использование информационных ресурсов Института;
- введение системы контроля и процедур по защите информации в структурных подразделениях Института, в информационных системах и сетях.

1.4. Область применения настоящего Положения распространяется на все подразделения Института, на всех сотрудников института, а также лиц, работающих по договорам гражданско-правового характера.

1.5. Нормативно-правовые документы, регламентирующие политику ИБ в Институте:

- Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 27.12.2019) «Об информации, информационных технологиях и о защите информации»;
- Методический документ ФСТЭК России от 11.02.2014 г. «Меры защиты информации в государственных информационных системах»;
- ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения;
- ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

2. ДОСТУП К ИНФОРМАЦИОННЫМ РЕСУРСАМ

2.1. Получение пользователями доступа к информационным ресурсам основывается на аутентификации пользователей и разграничении доступа.

2.2. В качестве объектов доступа рассматриваются информационные ресурсы Института, в отношении которых Институт имеет права владения, распоряжения, пользования: данные (информация), технические средства, программные средства, услуги (сервисы) информационных систем.

2.3. Каждому пользователю сопоставляется учетная запись и права доступа – с учетом их важности для деятельности Института.

2.4. Перед началом работы в информационных системах Института сотрудники, студенты и аспиранты проходят процедуру авторизации в Информационно-аналитическом управлении (ИАУ), где получают логины и пароли для доступа к информационным системам и ресурсам Института.

2.5. Доведение правил работы в информационных системах до персонала всех уровней проводится: при приеме на работу; в ходе совещаний, собраний, профессиональной подготовки персонала, тренингов по информационной безопасности; с помощью сайта, электронной почты и других технических средств.

2.6. Запрещается передача паролей третьим лицам, а также хранение паролей в местах, где они могут быть доступны.

2.7. При увольнении сотрудника обеспечивается невозможность его доступа к информационным ресурсам и системам Института.

3. ДОСТУП К РЕСУРСАМ СЕТИ ИНТЕРНЕТ

3.1. Доступ к сети Интернет должен быть разрешен только для выполнения служебных обязанностей и не может использоваться для ненадлежащей или незаконной деятельности.

3.2. При работе в сети Интернет запрещается передавать информацию ограниченного доступа (персональные данные, коммерческая и служебная информация) без соответствующего разрешения и надлежащей защиты (шифрование, пароли, электронная подпись).

3.3. При использовании сети Интернет в Институте необходимо соблюдать законодательные, регулирующие и контрактные требования в отношении авторских и смежных прав на интеллектуальную собственность в области программного обеспечения, а также в отношении научных и других материалов.

3.4. Запрещается посещать ресурсы сети Интернет, противоречащие законодательству РФ.

3.5. Лица, ответственные за обеспечение и контроль доступа в сеть Интернет, могут временно заблокировать доступ в сеть Интернет для пользователей, допустивших нарушения данного Положения.

4. ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ

4.1. Доступ сотрудника к корпоративной электронной почте Института должен быть санкционирован непосредственным руководителем.

4.2. Получение или смена адреса электронной почты для сотрудника обеспечивается ответственным лицом ИАУ после получения заявки от руководителя подразделения.

4.3. При использовании электронной почты в Институте запрещается передавать информацию ограниченного доступа (персональные данные, коммерческая и служебная информация) без соответствующего разрешения и надлежащей защиты (шифрование, пароли, электронная подпись).

4.4. При увольнении работника доступ к его электронной почте блокируется. Удаление адреса и содержимого электронной почты уволенного работника производится ответственным лицом ИАУ.

4.5. При нарушении указанных в данном Положении правил работы с электронной почтой доступ сотрудника к электронной почте может быть временно приостановлен ответственными лицами до устранения нарушения.

5. ИСПОЛЬЗОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

5.1. В Институте разрешается использовать следующие виды программного обеспечения (ПО):

- разработанное в Институте для обеспечения уставной деятельности Института;
- законно приобретенное или полученное Институтом на основании договорных или лицензионных соглашений с разработчиком либо правообладателем;
- «свободное» ПО, распространяемое с открытым исходным кодом (Open Source) либо под свободными лицензиями: GPL, LGPL, BSD, Apache и аналогичными;

- «бесплатное» ПО, лицензия на которое явно допускает его безвозмездное использование в корпоративной среде (в коммерческих целях, на служебных компьютерах, для выполнения должностных обязанностей и т.п.).

5.2. Доступ пользователей к системному и прикладному ПО должен быть санкционирован непосредственным руководителем только для выполнения служебных обязанностей.

5.3. Пользователям запрещено**:**

- приносить, скачивать, устанавливать и использовать нелицензионное программное обеспечение;
- использовать программное и аппаратное обеспечение Института в неслужебных (личных) целях;
- устанавливать и использовать программное обеспечение, которое не требуется для выполнения им должностных обязанностей.

5.4. ПО, установленное или используемое в Институте в нарушение настоящего Положения, может быть заблокировано или удалено ответственными лицами.

5.5. Средства защиты от вредоносного программного обеспечения (ВПО) должны быть установлены, настроены и активизированы на всех допускающих такую установку программно-технических средствах до начала их работы с информационными системами Института.

5.6. Средства защиты от ВПО должны иметь все последние обновления, полученные из доверенных источников.

5.7. Контролю на предмет обнаружения ВПО должна подвергаться вся информация, создаваемая и (или) обрабатываемая программно-техническими средствами, а также принимаемая и (или) передаваемая с помощью средств телекоммуникаций.

6. ИСПОЛЬЗОВАНИЕ СРЕДСТВ БЕСПРОВОДНОГО ДОСТУПА

6.1. Беспроводной доступ к информационным системам и ресурсам Института для работников Института и командированных разрешается при соблюдении требований безопасности.

6.2. Беспроводной доступ для участников конференций, семинаров, мероприятий разрешается исключительно для выхода в сеть Интернет.

6.3. Логин и пароль для беспроводного доступа выдается:

- для сотрудников Института - по заявке руководителя подразделения;
- для участников конференций, семинаров, мероприятий – по заявке лица, ответственного за мероприятие;
- для командированных и третьих лиц, выполняющих работы на территории Института – по заявке руководителя соответствующего подразделения.

7. ОРГАНИЗАЦИЯ РАБОЧИХ МЕСТ

7.1. При приеме на работу, при смене рабочего места, при изменении должностных обязанностей сотрудника – руководитель подразделения оформляет заявку в произвольном виде на организацию рабочего места пользователя с указанием потребностей и направляет ее начальнику ИАУ.

7.2. Выполнение заявки на обеспечение или изменение доступа пользователя включает в себя назначение прав доступа к сетевым ресурсам локальной сети, сети Интернет, электронной почте Института, программному обеспечению и базам данных.

7.3. В случае необходимости закрытия доступа пользователю к информационным ресурсам, руководитель подразделения заранее направляет заявку системному администратору ИАУ. На основании этой заявки в течение одного рабочего дня блокируется учетная запись пользователя, а также закрывается доступ к сетевым ресурсам, информационным системам, электронной почте, сети Интернет.

7.4. В случае отсутствия на непродолжительное время на своем рабочем месте, пользователь должен заблокировать доступ к своему компьютеру, обеспечить отсутствие информации на экране (или завершить сеанс работы), а также предпринять соответствующие меры по защите конфиденциальной информации на физических носителях.

7.5. Применяемые меры по обеспечению безопасности при хранении физических носителей информации должны соответствовать категории хранимой на них информации.

7.6. Пользователям запрещается без согласования с руководством использовать на рабочих местах оборудование, которое не принадлежит Институту на правах собственности, аренды, пользования, либо в отношении которого Институт не обладает иными (в том числе неисключительными) правами.

8. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

8.1. Техническое обслуживание и ремонт оборудования и кабельных линий (электропитания и телекоммуникаций) производится только уполномоченными на это сотрудниками (персоналом соответствующих подразделений и обслуживающим персоналом).

8.2. Техническое обслуживание оборудования и кабельных линий проводится регулярно в соответствии с регламентом технического обслуживания.

8.3. Техническое обслуживание и ремонт оборудования и кабельных линий проводится таким образом, чтобы исключить или минимизировать риски потери функциональности корпоративной информационной системы.

8.4. В программно-технических средствах, направляемых для технического обслуживания и ремонта, вся конфиденциальная информация (данные и программы) после переноса на другие носители уничтожается способом, обеспечивающим невозможность ее восстановления.

8.5. Все устройства хранения информации перед утилизацией проверяются на наличие конфиденциальной информации. При наличии таковой, они уничтожаются способом, гарантирующим невозможность восстановления ранее хранящейся на них информации.

8.6. Выявленные в процессе технического обслуживания отклонения и неисправности регистрируются и устраняются немедленно либо (при необходимости) заносятся в план по ремонту.

8.7. Разработаны процедуры поддержки (восстановления) работы и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или отказа процессов, критичных для деятельности Института.

8.8. Все технические средства Института подлежат инвентаризации с документированием результатов в соответствующем реестре.

8.9. Ответственным лицом ИАУ регулярно проводится мониторинг информационной безопасности для выявления нецелевого использования средств обработки информации пользователями, несанкционированных действий сотрудников и авторизованных третьих лиц в корпоративной информационной системе Института, оперативного реагирования на инциденты информационной безопасности, сбора данных и проведения служебных расследований.

8.10. Расследование инцидентов (нарушений) информационной безопасности в Институте осуществляется в порядке, определенном действующим законодательством РФ и внутренними документами Института.

8.11. Все пользователи информационных систем, услуг и ресурсов Института должны сообщать о любых замеченных или подозреваемых недостатках безопасности в системах или услугах так оперативно, насколько это возможно.

9. ОТВЕТСТВЕННОСТЬ

9.1. Ответственность за соблюдение данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

9.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений Института; сотрудников ИАУ, ответственных за администрирование сегментов информационной телекоммуникационной системы Института; сотрудников, выполняющих функции администраторов информационных систем и администраторов локальной вычислительной сети.

10. КОНТРОЛЬ

10.1. Целью контроля ИБ является выявление угроз, предотвращение их реализации, минимизация возможного ущерба.

10.2. Объектами контроля ИБ являются информационные ресурсы Института (информация, работники и другие субъекты доступа, системы и средства информационных технологий, а также средства защиты информации).

10.3. Контроль соблюдения требований настоящего Положения возлагается на ответственное лицо, назначенное приказом ректора Института.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Все решения по изменению и дополнению настоящего Положения принимаются Ректором.

11.2. Настоящее Положение вступает в силу с момента подписания Ректором.