УТВЕРЖДЕНО
Приказ ректора
от 31.01.2024 № 171

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ ОБРАЗОВАНИЯ «ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ФРАНЦИСКА СКОРИНЫ»

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Политика информационной безопасности (далее – Политика) разработана на основании Конституции Республики Беларусь, Трудового кодекса Республики Беларусь, Закона Республики Беларусь «Об информации, информатизации и защите информации», Закона Республики Беларусь «О защите персональных данных» и иных нормативных правовых актов Республики Беларусь в области информационной безопасности.

1.2 Политика распространяется на работников и обучающихся в учреждении образования «Гомельский государственный университет имени Франциска Скорины» (далее – Университет), а также привлекаемых лиц, участвующих в эксплуатации (использующих в своей работе), обслуживании, поддержке объектов информационной системы (далее – ОИС), программного обеспечения (прикладного и системного) (далее – ПО), информационных ресурсов (далее – ИР), информационных систем (далее – ИС) Университета (собственных, либо предоставленных на договорной основе).

1.3 Общее руководство системой информационной безопасности (далее – ИБ), принятие всех решений по вопросам ее функционирования, а также контроль за организацией работы по обеспечению ИБ возлагается на ректора. На проректоров возлагается ответственность за обеспечение ИБ по направлениям в соответствии с распределением обязанностей.

1.4 Организационные и технические работы по обеспечению ИБ компьютерной сети и баз данных автоматизированных систем управления в Университете выполняет центр информационных технологий (далее – ЦИТ) в соответствии с локальными правовыми актами (далее – ЛПА), устанавливающими порядок осуществления деятельности по ИБ в Университете. Обеспечивается наличие лиц, обладающих необходимой квалификацией и прошедших соответствующее обучение, а также повышение квалификации в установленном порядке.

Глава 2. ПРИНЦИПЫ И ЦЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

2.1 Политика Университета по обеспечению ИБ направлена на гармонизацию подходов и требований по обеспечению ИБ для сотрудников и обучающихся Университета, государственных органов и организаций, а также юридических и физических лиц и индивидуальных предпринимателей (далее – субъекты информационных отношений) при осуществлении Университетом своей деятельности.

2.2 Основными целями Политики ИБ являются:

снижение уровня рисков, связанных с ИБ;

снижение числа инцидентов, связанных с ИБ;

повышение компетентности персонала в области ИБ;

улучшение имиджа Университета и минимизация ущерба вследствие возможного возникновения инцидентов ИБ и кибербезопасности;

обеспечение непрерывности бизнес-процессов;

обеспечение соответствия требованиям законодательства, стандартам и договорным обязательствам в части ИБ и защиты персональных данных.

2.3 Достижение указанных целей осуществляется посредством выполнения следующих мероприятий:

реализация требований законодательства Республики Беларусь в части ИБ и мер контроля их защищенности;

определение ответственности субъектов информационных отношений (далее – Субъектов) по обеспечению и соблюдению требований Политики, в том числе с использованием ИР, ИС и ОИС, а также посредством принятия соответствующих внутренних ЛПА по обеспечению ИБ Университета;

своевременное выявление и оценка причин, условий и характера угроз ИБ, а также дальнейшее прогнозирование развития событий на основе мониторинга инцидентов ИБ;

планирование, реализация и контроль эффективности использования мер и средств защиты информации, создание механизма оперативного реагирования на угрозы ИБ;

повышение осведомленности и обучение сотрудников Университета возможным факторам рисков ИБ и мерам противодействия им.

2.4. Построение системы защиты информации и ее функционирование должно осуществляться в соответствии со следующими принципами:

законность: предполагает осуществление защитных мероприятий и разработку системы защиты информации Университета в соответствии с действующим законодательством Республики Беларусь;

системность: системный подход к построению системы защиты информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации;

комплексность: комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты;

непрерывность защиты: непрерывный, целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем;

своевременность: предполагает упреждающий характер мер для обеспечения безопасности информации;

преемственность и совершенствование: предполагают постоянное совершенствование мер и средств защиты информации;

экономическая целесообразность: предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов по отношению к величине возможного ущерба;

персональная ответственность: предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого работника в пределах его полномочий;

принцип минимизации полномочий: означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью;

простота применения средств защиты: механизм защиты должен быть интуитивно понятен и прост в использовании, без значительных дополнительных трудозатрат;

научная обоснованность и техническая реализуемость: информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации;

контроль: предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил безопасности.

Глава 3. СУБЪЕКТЫ, ОБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ И ПОРЯДОК ИХ ВЗАИМОДЕЙСТВИЯ

3.1 Субъектами информационных отношений являются:

Университет, выступающий в качестве владельца информации и собственника имеющихся ИР, ИС и ОИС;

государственные органы и организации;

физические и юридические лица (индивидуальные предприниматели), в том числе иностранные, международные организации, выступающие в качестве информационных посредников, операторов информационных систем и связи, поставщиков ОИС, а также в качестве поставщика услуг Университету, в том числе технической поддержки, гарантийного и сервисного обслуживания.

3.2 Субъектами в рамках Университета являются внутренние и внешние пользователи:

внутренние пользователи:

работники ЦИТ, осуществляющие обеспечение безопасного использования ИР, ИС и ОИС;

персонал и профессорско-преподавательский состав Университета, получивший доступ к ИР, ИС и ОИС предприятия и использующий их в рамках выполнения своих должностных обязанностей;

внешние пользователи:

посетители Университета;

должностные лица организаций, поставляющие ИР, ИС и ОИС для Университета и осуществляющие их гарантийное и сервисное обслуживание.

3.3 Ответственность Субъектов информационных отношений за обеспечение защиты информации в Университете установлена в следующих документах:

организационно-распорядительных документах;

должностных инструкциях работников (для внутренних пользователей);

иных документах, в том числе соглашениях и договорных обязательствах при оказании услуг.

3.4 Объектами информационных отношений (далее – Объекты) являются:

информация, хранящаяся и обрабатываемая в информационных системах Университета, в том числе конфиденциальная и содержащая персональные данные;

информационная инфраструктура, включающая ИР, ИС и ОИС.

3.5 Порядок информационного взаимодействия Объектов между собой определяется соответствующей эксплуатационной (технической) документацией.

3.6 Основными составляющими Объектами являются компоненты, входящие в состав информационной инфраструктуры Университета:

локальной вычислительной сети;

информационных систем;

отдельных рабочих мест, предназначенных для доступа, хранения и обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Глава 4. РАЗГРАНИЧЕНИЕ ДОСТУПА К ОБЪЕКТАМ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

4.1 Субъекты имеют необходимый уровень доступа к Объектам Университета, назначенный в соответствии с принципом минимизации прав, назначаемых пользователям (это означает

предоставление пользователям минимальных прав доступа в соответствии с должностными обязанностями). Доступ к информации и настройкам предоставляется только в том случае и объеме, если это необходимо пользователю для выполнения его должностных обязанностей:

работникам ЦИТ предоставляется доступ к Объектам в соответствии с их ответственностью и полномочиями;

персоналу Университета и профессорско-преподавательскому составу предоставляется доступ к Объектам в рамках выполнения ими соответствующих должностных обязанностей;

лицам, поставляющим ОИС, а также осуществляющим их гарантийное, сервисное обслуживание и жизнеобеспечение, предоставляется доступ к Объектам в рамках договорных отношений на оказание услуг;

в рамках Заявлений и Соглашений;

в рамках документов системы менеджмента качества;

посетителям Университета и обучающимся предоставляются исключительно гостевой доступ к сетям, либо устройствам, с ограниченным доступом к ИС и ИР Университета.

4.2 Порядок и правила предоставления доступа к Объектам Университета определяются следующими документами:

настоящей политикой;

договорными отношениями при оказании ГГУ имени Ф. Скорины услуг, в том числе технической поддержки;

должностными инструкциями работников;

положением о ЦИТ;

иными локальными нормативными актами Университета.

4.3 Делопроизводство по документам, содержащим служебную информацию ограниченного распространения, регулируется существующим законодательством и ЛПА, содержащим служебную информацию ограниченного распространения.

4.4 Разграничение доступа к ИС и их Объектам осуществляется с помощью средств управления правами доступа к соответствующим активам. К указанным средствам относятся:

групповые политики безопасности;

средства управления доступом к ОС;

средства управления доступом к официальному сайту Университета и электронной почте;

средства управления доступом к ИС, ИР, ОИС Университета;

средства управления доступом к базам данных Университета;

средства управления доступом к системам хранения данных Университета;

средства управления доступом к ИС и их Объектам, ИР, предоставленным пользователям в рамках выполнения должностных обязанностей и договорных отношений.

4.5 Разграничение доступа к вышеуказанным активам предприятия включает в себя:

регистрацию и идентификацию пользователей;

аутентификацию пользователей;

авторизацию пользователей для получения доступа;

регистрацию и учет попыток доступа к защищаемым активам.

4.6 При определении полномочий каждого авторизованного пользователя выполняются следующие условия:

полномочия пользователя соответствуют его должностным обязанностям и осуществляются только в границах этих полномочий;

полномочия пользователя должны распространяться на конкретные категории информации, ИС и их Объектов, ИР.

4.7 С целью разграничения прав доступа работников к Объектам Университета используются роли безопасности. В базовом варианте применяются следующие роли безопасности: роль «Администратор» и «Пользователь». В случае необходимости более

детального разграничения применяются дополнительные роли, в зависимости от конкретной ИС и ИР.

4.8 Назначение ролей пользователей информационной инфраструктуры Университета осуществляется исходя из выполняемых ими должностных обязанностей. Для каждой роли в отношении единицы актива определен и\или ограничен список допустимых операций. Допускается совмещение нескольких ролей одним работником по функциям, не оказывающим влияния на уровень безопасности объекта, в том случае, если эти роли не являются взаимоисключающими.

Каждой роли соответствуют определенные права доступа Субъекта к Объекту – авторизованный пользователь. Ролевое деление авторизованных пользователей реализуется с помощью функциональных возможностей разграничения доступа к ИС и их Объектам, ИР.

В случае предоставления пользователю новой роли его права доступа к защищаемым данным и информационной инфраструктуре Университета пересматриваются.

В случае увольнения или перевода работника Университета в другое структурное подразделение либо на другую должность его права доступа пересматриваются или блокируются.

В случае выявления инцидентов безопасности права доступа авторизированного пользователя блокируются (либо ограничиваются) до завершения рассмотрения инцидента.

4.9 ОИС (за исключением ПК и мобильных устройств, используемых в служебных целях вне территории Университета) располагаются в помещениях, исключающих несанкционированный доступ к ним и обеспечивающих их бесперебойную круглосуточную эксплуатацию в климатических условиях, указанных в документации на эксплуатацию.

4.10. Сотрудникам структурных подразделений, имеющим право доступа к обработке персональных данных, содержащихся в информационных системах (ресурсах) Университета, обеспечивается право доступа к соответствующим ИС.

Глава 5. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ (ПОЛЬЗОВАТЕЛЕЙ) ИНФОРМАЦИОННЫХ СИСТЕМ

5.1 Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании Объектов информационных отношений имеют право:

использовать ОИС для доступа к ИС и ИР, другим ОИС с целями поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления и пользования информацией;

осуществлять иные действия в соответствии с должностными инструкциями и ЛПА Университета.

5.2 Субъекты информационных отношений в пределах предоставленных им полномочий и (или) прав при использовании Объектов информационных отношений обязаны:

соблюдать права других лиц при использовании Объектов Университета;

исполнять обязанности в соответствии с должностными инструкциями и ЛПА Университета.

5.3 Права и обязанности субъектов Университета регламентированы следующими документами:

настоящей Политикой;

Положением об обработке и защите персональных данных;

Положением о ЦИТ;

должностными инструкциями работников Университета.

5.4 Университет обязуется постоянно совершенствовать систему ИБ, обеспечивать ресурсами, достаточными для достижения указанных в настоящей Политике целей.

Глава 6. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ ОБЪЕКТОВ УНИВЕРСИТЕТА С ИНЫМИ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И СИСТЕМАМИ

6.1 Порядок взаимодействия Объектов Университета с иными ИС определяется действующим законодательством и соответствующими документами по каждому взаимодействию.

6.2 Функционирование Объектов Университета осуществляется с обновлением системного, прикладного ПО и антивирусных баз из доверенных источников.

6.3 Обновление баз средств защиты информации от действий вредоносного ПО и файлов осуществляется с периодичностью, установленной производителем антивирусного ПО.

6.4 Доступ к сети Интернет предоставляется только авторизованным сервисам и пользователям.

6.5 К авторизованным сервисам Университета относятся:

обновление системного и прикладного ПО;

обновление встроенного ПО технических средств;

обновление баз средств защиты информации от действий вредоносного ПО и файлов.

6.6 Правила доступа к сетям общего пользования определены и регулируются настоящей Политикой.

6.7 При взаимодействии Объектов Университета с иными ИС, в случае необходимости, применяются средства защиты информации, имеющие сертификат соответствия, выданный в порядке, установленном законодательством.

Глава 7. ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ

7.2 Персональная ответственность за соблюдение требований настоящей Политики в структурных подразделениях Университета возлагается на их руководителей, а также проректоров по курируемым направлениям в соответствии с распределением обязанностей.

7.3 Неисполнение или некачественное исполнение работниками Университета, обучающимися, пользователями ИС обязанностей по обеспечению ИБ может повлечь лишение доступа к информационным ресурсам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в Университете порядком либо требованиями действующего законодательства.

Глава 8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1 В случае изменения действующего законодательства и иных нормативных актов, Устава Университета настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Университета. В этом случае ответственное лицо обязано незамедлительно инициировать внесение соответствующих изменений.

8.2 Ответственным за внесение изменений и дополнений в настоящую Политику является начальник ЦИТ университета.

8.3 Изменения в Политике информационной безопасности согласовываются с первым проректором Университета, проректором по безопасности, режиму и кадрам, после чего утверждаются ректором.