Федеральное агентство морского и речного транспорта

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Государственный университет морского и речного флота имени адмирала С.О. Макарова»

Политика информационной безопасности

Санкт-Петербург
2023

СТРАНИЦА СТАТУСА ДОКУМЕНТА

Приложение № 1

к приказу ФГБОУ ВО «ГУМРФ
имени адмирала С.О. Макарова»
от 29.05. 2023 № 601

Система менеджмента качества **Политика информационной безопасности**	Новая редакция
	Дата введения - в соответствии с приказом

Настоящая политика информационной безопасности разработана согласно требованиям Международного Стандарта ИСО 9001-2015 и является документом системы менеджмента качества ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова. Политика информационной безопасности разработана в соответствии с действующим законодательством и нормативными правовыми актами Российской Федерации. Настоящая политика информационной безопасности выражает позицию руководства ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» в отношении путей и способов обеспечения необходимого уровня информационной безопасности.

Контроль документа	Первый проректор
Руководитель разработки	Директор департамента цифрового развития и информатизации Кислов Р.И.
Исполнитель	Кислов Р.И.

Оглавление

Лист ознакомления

№	Должность	Ф.И.О.	Дата	Подпись
1				
2				
3				
4				
5				
6				

Лист учета экземпляров

Место хранения корректируемых экземпляров	№ экземпляра
Департамент цифрового развития и информатизации	2

Место хранения некорректируемого экземпляра	№ экземпляра
Общий отдел	1
Служба качества	3
Корпоративный портал	4

Лист учета корректуры

№	Номер страницы	Номер пункта	Изменение (проверка)	Дата внесения корректуры (проверки)	Утверждение корректуры (Ф.И.О. / Подпись)

I. Общие положения

1.1. Применение современных информационных технологий в повседневной деятельности является необходимым условием устойчивого и эффективного функционирования университета. Информационные активы, которыми располагает университет, представляют для него реальную ценность. Поэтому информационные активы, наряду с ИТ-инфраструктурой, нуждаются в адекватной защите от рисков, способных вызвать негативные последствия для функционирования университета.

1.2. Политика информационной безопасности (далее - Политика ИБ) выражает позицию руководства университета в отношении путей и способов обеспечения необходимого уровня информационной безопасности.

3.1. Положения Политики ИБ являются основой для принятия управленческих решений по надлежащей защите информационных активов университета и контролю их исполнения.

3.2. Политика ИБ формулирует базовые принципы и положения, следуя которым университет создает и поддерживает ИТ-инфраструктуру в состоянии, обеспечивающем конфиденциальность, целостность и доступность информационных активов.

3.3. На основе требований Политики ИБ университет разрабатывает и внедряет систему нормативных и организационно-распорядительных и эксплуатационных документов, регулирующих различные аспекты обеспечения информационной безопасности и осуществляет внедрение выбранных технологий обеспечения ИБ, позволяющих достичь требуемого уровня защиты информационных активов и ИТ-инфраструктуры.

II. Термины и определения

2.1. Университет - Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова».

2.2. ИС – Информационные системы.

2.3. Информационный актив (информация) – данные, сведения, обрабатываемые в университете с помощью ИС.

2.4. Владельцы информационных активов (информации) – руководители подразделений университета, в которых создаются, обрабатываются и хранятся информационные активы.

2.5. Конфиденциальность – защищенность информационных активов от несанкционированного доступа.

2.6. Целостность – способность сохранить неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2.7. Доступность информации – свойство информации, заключающееся в возможности ее получения авторизованным пользователем в нужное для него время.

2.8. Меры информационной безопасности (ИБ) – комплекс мер по обеспечению целостности, доступности и конфиденциальности информационных активов, создаваемых, хранимых, обрабатываемых и передаваемых внутри университета и/или за его пределами.

2.9. Политика – документ, определяющий позицию руководства университета и формирующий требования в отношении обеспечения ИБ. Детализированное описание способов выполнения требований, изложенных в политиках, определено в соответствующих процедурах и положениях.

2.11. Информационная инфраструктура университета - совокупность сетей передачи данных, серверов, системного и прикладного программного обеспечения, ИС, персональных компьютеров, систем защиты информации и контроля защищенности информации.

2.12. АСУ «Университет» – автоматизированная система управления, предназначенная для контроля учебного процесса, управления образовательной и научной деятельностью университета.

2.13. РИТКС – распределенная информационно-телекоммуникационная сеть университета.

2.14. Пользователи – администраторы ИС, работники университета или сторонней организации, которым предоставлен доступ к ИС университета.

2.15. Нормативные документы ИБ – политики, процедуры (регламенты), стандарты и инструкции, выражающие позицию и требования университета в области информационной безопасности, а также способы выполнения этих требований.

2.16. Угроза – причина осуществления нежелательных событий, способных нанести ущерб университету.

2.17. Риск – ущерб в единицу времени, который может понести университет в случае реализации угрозы.

2.18. Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры университета в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

2.19. Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта информационной инфраструктуры университета и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

III. Область действия

3.1. Политика ИБ распространяется на все структурные подразделения и все филиалы университета, всех работников и обучающихся университета, а также на работников сторонних организаций, имеющих доступ к информационным активам университета.

3.2. Политика ИБ распространяется на все информационные активы университета, обеспечивая через внедрение в практику сформулированных принципов и положений, их защиту от нарушения целостности, конфиденциальности и доступности, а также защиту ИТ-инфраструктуры от разрушения, повреждения, вредоносных воздействий, хищения или модификации ее элементов.

IV. Принципы и направления обеспечения информационной безопасности университета

4.1. Реализация Политики ИБ университета должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информационных активов не только с помощью одного отдельного средства (мероприятия),но и с помощью их простой совокупности. Необходимо их системное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы университета должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий. Руководство университета принимает все необходимые экономически обоснованные мерыдля достижения требуемого уровня защиты.

4.2. Предпринимаемые меры информационной безопасности должны быть направлены на обеспечение необходимого, с точки зрения законодательства, уровня конфиденциальности, целостности и/или доступности информационных активов,

обеспечение устойчивости функционирования информационной инфраструктуры университета.

4.3. Основными направлениями реализации Политики ИБ университета являются:

- обеспечение защиты информационных активов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий (защита от НСД);
- недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование объектов информационной инфраструктуры;
- восстановление функционирования объектов информационной инфраструктуры, в том числе за счет создания и хранения резервных копий необходимой для этого информации;
- обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и при передаче по каналам связи.

4.4. Положения настоящей Политики ИБ университета уточняются (дополняются) политиками ИБ объектов информационной инфраструктуры, учитывающих функциональные и иные особенности этих объектов. Политики ИБ объектов информационной инфраструктуры являются нормативными документами второго уровня.

4.5. Университет защищает информационные активы, представленные как в электронном виде, так и в виде твердых копий: на бумажных, магнитных, оптических и иных типах носителей информации.

4.6. Обеспечение ИБ на объектах информационной инфраструктуры университета осуществляется по следующим направлениям:

- управление ИБ;
- идентификация и категорирование информационных активов;
- организация работы с персоналом по вопросам ИБ;
- реагирование на инциденты ИБ;
- обеспечение непрерывности учебно-образовательных процессов;
- обеспечение ИБ при эксплуатации средств обработки, хранения и передачи информации и использования информационных активов;
- защита технических средств и систем;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению безопасности;
- управление конфигурацией;
- аудит безопасности;
- информирование и обучение персонала;
- обеспечение соответствия требованиям по ИБ.

Данные направления реализуются организационными и техническими мерами.

4.7. Необходимые меры ИБ должны быть предприняты на всех этапах жизненного цикла объектов информационной инфраструктуры – создания, хранения, эксплуатации и вывода из эксплуатации.

4.8. Заявленные положения политики ИБ развиваются и детализируются в отдельных документах: политиках, процедурах (регламентах), инструкциях в области обеспечения информационной безопасности

V. Управление информационной безопасностью

5.1. Организационную структуру системы управления информационной безопасностью Университета образуют:

- первый проректор;

- директор департамента цифрового развития и информатизации;
- управление безопасности;
- руководители структурных подразделений Университета;
- ответственные за обеспечение безопасности информации, назначаемые в филиалах университета;
- исполнители, допущенные к работам и документам, связанным с обработкой информации, подлежащей защите (в соответствии со специальными обязанностями по безопасности информации).

5.2. Система управления информационной безопасности университета должна обеспечивать:

- проведение единой технической политики, организацию и координацию работ по защите информации;
- проведение, в пределах своей компетенции, проверочных мероприятий и контроля эффективности применения мер защиты информации.

5.3. Общую координацию работ по защите информационных активов университета, осуществляет директор департамента цифрового развития и информатизации.

5.4. Непосредственное управление системой информационной безопасности университета возлагается на первого проректора. Решения первого проректора по вопросам защиты информации являются обязательными к исполнению всеми структурными подразделениями и должностными лицами, выполняющими работы, связанные с обработкой защищаемой информации.

5.5. Практическая реализация целей защиты информации, в части создания и обеспечения эффективности функционирования системы защиты информации в университете, возлагается на отдел сетевого и системного администрирования департамента цифрового развития и информатизации. Задачи и функции отдела регламентируются Положением об отделе сетевого и системного администрирования департамента цифрового развития и информатизации.

5.6. Руководство университета предоставляет директору департамента цифрового развития и информатизации все необходимые полномочия для принятия требуемых действий по обеспечению адекватного уровня ИБ.

5.7. Функции администрирования и контроля средств защиты информации в филиалах выполняются ответственными за обеспечение безопасности информации, назначаемыми по согласованию с первым проректором из числа работников подразделений, эксплуатирующих объекты информационной инфраструктуры. Указанные работники осуществляют свою деятельность на основании соответствующих инструкций и специальных обязанностей по обеспечению безопасности информации.

5.8. Администрирование ИБ направлено на обеспечение выполнения установленных правил доступа к объектам информационной инфраструктуры, порядка обращения с защищаемой информацией при ее обработке, хранении, передаче.

На отдел сетевого и системного администрирования возлагается ответственность по предотвращению несанкционированного доступа к защищаемой информации.

Для реагирования на компьютерные инциденты определяются работники из числа работников департамента цифрового развития и информатизации, ответственные за выявление компьютерных инцидентов и реагирование на них, и определяются их функции.

5.9. В университете ежегодно разрабатывается план мероприятий по обеспечению ИБ на будущий год, в том числе мероприятий по контролю состояния ИБ.

VI. Идентификация и категорирование информационных активов

6.1. В целях обеспечения ИБ в университет осуществляется идентификация и категорирование информационных активов в соответствии с требованиями законодательства.

6.2. Идентифицированные и категорированные информационные активы отражаются в инвентаризационной документации, маркируются и для них назначаются владельцы – работники университета ответственные за обеспечение ИБ информационных активов.

6.3. Процедуры повторяются ежегодно. Внеплановые процедуры идентификации и категорирования информационных активов выполняются в случае внесения существенных изменений в информационную инфраструктуру университета.

6.4. На основании результатов категорирования информационных активов определяются применяемые по отношению к ним меры безопасности.

6.5. Процедуры обработки информации и правила использования информационных активов определяются настоящей Политикой, а также другими нормативными и организационно-распорядительными документами университета в области ИБ.

VII. Организация работы с персоналом по вопросам информационной безопасности

7.1. Обеспечение безопасности при заключении и во время действия трудового договора.

В целях повышения уровня информационной безопасности при приеме на работу новых работников осуществляется доведение до них правил информационной безопасности и устанавливается ответственность за их нарушение.

Обязанности работников университета по соблюдению правил ИБ определяются нормативными и организационно-распорядительными документами университета в области ИБ, также работники подписывают обязательства о соблюдении режима конфиденциальности персональных данных (Приложение 1).

7.2. Для работников университета реализуются мероприятия повышения осведомленности в области ИБ.

Работники, отвечающие за обеспечение ИБ, регулярно проходят повышение квалификации, знакомятся с изменениями в федеральном законодательстве в области ИБ.

7.3. Работники университета, имеющие доступ к информации подлежащей защите, несут ответственность за ее разглашение и утрату, а также за нарушение установленного порядка обеспечения ИБ.

Работники, разгласившие подлежащую защите информацию или нарушившие установленный порядок обращения с ней, а также работники по вине которых произошла ее утрата или искажение, несут ответственность в соответствии с действующим законодательством Российской Федерации.

7.4. В целях обеспечение ИБ при увольнении и изменении условий трудового договора в университете осуществляется контроль возврата технических средств обработки, хранения и передачи информации, своевременного прекращения прав доступа работников к информационным активам университета.

7.5. При увольнении работника (изменении условий трудового договора) его права доступа к информационным активам незамедлительно аннулируются (приводятся в соответствие с новыми условиями).

VIII. Управление инцидентами информационной безопасности

8.1. В целях предотвращения нарушений ИБ в университете принимаются меры к оповещению об инцидентах информационной безопасности.

8.2. Работники университета обязаны сообщать в департамент цифрового развития и информатизации о любых замеченных или предполагаемых нарушениях безопасности информации, а также выявленных уязвимостях в соответствии с установленным в университете порядке.

8.3. В целях реагирования на инциденты ИБ осуществляется их регистрация и анализ, а также принятие необходимых мер по исключению их повторения.

8.4. Ответственным за реагирование на инциденты ИБ является начальник отдела сетевого и системного администрирования департамента цифрового развития и информатизации.

IX. Порядок обеспечения информационной безопасности на этапах жизненного цикла объектов информационной инфраструктуры

9.1. Информационная безопасность информационной инфраструктуры университета обеспечивается на всех стадиях жизненного цикла ее объектов с учетом ролей всех вовлеченных в этот процесс сторон (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих организаций и надзорных органов).

9.2. Жизненный цикл объекта информационной инфраструктуры университета включает в себя следующие этапы:

- обоснование требований к объекту;
- разработка (модернизация) объекта;
- ввод объекта в действие;
- эксплуатация объекта;
- вывод объекта из эксплуатации.

9.3. Департамент цифрового развития и информатизации в части сопровождения вопросов ИБ участвует во всех этапах жизненного цикла объектов информационной инфраструктуры университета.

9.4. Порядок разработки требований к информационной инфраструктуре университета регламентируется нормативными и организационно-распорядительными документами университета.

X. Обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных активов

10.1. Физическая защита объектов информационной инфраструктуры университета.

В целях предотвращения несанкционированного доступа к объектам информационной инфраструктуры университета обеспечивается физическая защита мест их эксплуатации (размещения).

Технические средства обработки, хранения и передачи информации размещаются в запираемых шкафах, располагаемых в специализированных помещениях, доступ посторонних лиц к которым ограничивается.

Порядок обеспечения физической защиты объектов информатизации определяется их политиками ИБ.

10.2. Защита территорий, зданий и помещений университета.

В целях обеспечения защиты информации и технических средств обработки, хранения и передачи информации обеспечивается защита территорий, зданий и помещений университета.

В университете устанавливается пропускной режим, препятствующий бесконтрольному посещению его охраняемых территорий и зданий. Порядок посещения и поведения в зданиях и помещениях университета регламентируется нормативными и организационно-распорядительными документами университета в области ИБ.

Здания и помещения университета обеспечиваются техническими средствами охраны, системами контроля доступа и пожарной безопасности.

10.3. Для защиты информации ограниченного доступа во время проведения переговоров и иных мероприятий конфиденциального характера в университете выделяются защищаемые помещения, в которых обеспечивается защита информации от несанкционированного прослушивания и утечки по техническим каналам. Доступ в защищаемые помещения строго контролируется.

При проведении работ на охраняемых территориях университета, в его зданиях и защищаемых помещениях третьими лицами обеспечивается контроль их деятельности.

10.4. Порядок защиты помещений, в которых располагаются технические средства (серверы, централизованные хранилища данных, сетевое оборудование и средства защиты информации) определяется нормативными и организационно-распорядительными документами университета в области ИБ.

10.5. В целях обеспечения ИБ объектов информационной инфраструктуры в университете устанавливаются правила безопасной эксплуатации средств обработки, хранения и передачи информации.

Принимаются меры по обеспечению использования средств обработки, хранения и передачи информации только по целевому назначению.

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на специально выделенных для этого работников.

Правила эксплуатации средств обработки, хранения и передачи информации, используемых в университете, определяются политиками ИБ объектов защиты.

10.6. В целях предотвращения проникновения, обнаружения и нейтрализации вредоносного ПО в университете создается система защиты информационной инфраструктуры университета от вредоносного ПО.

Архитектура системы защиты от вредоносного ПО обеспечивает многоуровневую (эшелонированную) защиту.

10.7. В целях обеспечения возможности восстановления информационных активов в случае их утраты или нарушения целостности в университете осуществляется их резервное копирование.

Способ и периодичность резервного копирования, сроки хранения резервных копий определяются в зависимости от назначения и особенностей системы, в которой информация обрабатывается, а также от ценности информации.

Порядок резервного копирования информационных активов определяется нормативными и организационно-распорядительными документами университета в области ИБ.

10.8. В целях обеспечения бесперебойного функционирования информационной инфраструктуры университета осуществляется резервирование средств обработки, хранения и передачи информации, влияющих на непрерывность функционирования информационной инфраструктуры.

10.9. Обеспечение сетевой безопасности достигается защитой распределенной информационно-телекоммуникационной сети (РИТКС) университета, сетевых сервисов АСУ «Университет» и сетевой инфраструктуры филиалов и учебных городков. Порядок обеспечения сетевой безопасности определяется соответствующими политиками ИБ, а также другими нормативными и организационно-распорядительными документами университета в области ИБ.

10.10. В целях предотвращения разглашения, утечки или утраты информации в университете применяются меры защиты съемных носителей информации.

Осуществляется мониторинг использования съемных носителей. Утилизация неиспользуемых носителей осуществляется только с обеспечением гарантированного уничтожения содержащейся на них информации.

Порядок обеспечения ИБ при обращении со съемными носителями информации определяется нормативными и организационно-распорядительными документами университета в области ИБ.

10.11. В целях предотвращения разглашения, утечки или утраты информации в университете применяются меры по защите информации при ее передаче различными методами.

Порядок защиты обмена информацией определяется политиками ИБ объектов защиты, а также другими нормативными и организационно-распорядительными документами университета в области ИБ.

10.12. В целях поддержания работоспособности ПО в университете осуществляются меры по устранению уязвимостей ПО, а также другие меры защиты.

Устранение уязвимостей ПО достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками ПО. Новое ПО и все обновления принимаются в эксплуатацию только после успешного прохождения тестирования. Обновление ПО возлагается на департамент цифрового развития и информатизации.

10.13. В целях своевременного выявления нарушений ИБ в университете осуществляется контроль событий ИБ.

В университете осуществляется регистрация и учет в журналах событий технических средств обработки, хранения и передачи информации событий, которые могут быть связаны с нарушениями ИБ. Журналы событий регулярно анализируются работниками отдела сетевого и системного администрирования департамента цифрового развития и информатизации. Результаты регистрации и учета событий используются при проведении мероприятий по управлению инцидентами ИБ.

10.14. В целях своевременного и эффективного реагирования на опубликованные и выявленные уязвимости, а также устранения недостатков в конфигурации технических средств обработки, хранения и передачи информации в информационной инфраструктуре университета принимаются меры контроля защищенности.

Контроль защищенности осуществляется работниками отдела сетевого и системного администрирования департамента цифрового развития и информатизации. Перечень объектов контроля защищенности определяется порезультатам идентификации и категорирования информационных активов.

10.15. В целях обеспечения конфиденциальности, целостности и аутентичности обрабатываемой, хранимой и передаваемой информации в информационной инфраструктуре университета применяются сертифицированные установленным порядком криптографические средства защиты.

Электронные документы, для которых необходимо обеспечить целостность и аутентичность защищаются с помощью электронной цифровой подписи.

При передаче информации ограниченного доступа вне контролируемых зон, в том числе при использовании беспроводных сетей, применяются средства криптографической защиты информации.

При использовании мобильных устройств информация ограниченного доступа, хранимая на них, защищается с использованием криптографических средств защиты.

Порядок применения средств криптографической защиты определяются приказом ректора об обращении со средствами криптографической защиты информации и прилагающимися к нему:

- инструкцией по обращению со средствами криптографической защиты информации (СКЗИ),
- инструкцией ответственного за организацию работ по криптографической защите информации,
- инструкцией пользователей средств криптографической защиты информации.

XI. Контроль доступа

11.1. Управление доступом пользователей

В целях обеспечения безопасности и устойчивого функционирования информационной инфраструктуры в университете осуществляется управление доступом пользователей к ее информационным активам, прикладным системам и соответствующим техническим средствам объектов защиты.

Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями основывается на их должностных обязанностях. При этом используется принцип ролевого управления доступом. Права доступа и привилегии пользователей подлежат регулярному пересмотру.

Порядок управления доступом пользователей определяется настоящей Политикой ИБ, Положением о персональных данных, а также другими нормативными и организационно-распорядительными документами университета в области ИБ.

11.2. Ответственность пользователей.

В целях предотвращения несанкционированного доступа, а также компрометации или утраты информации и средств обработки информации, определяется ответственность пользователей по соблюдению правил доступа при использовании автоматизированных рабочих мест (АРМ).

Пользователи несут ответственность за соблюдение установленных правил при выборе и использовании паролей. Парольная политика и правила использования паролей определяются нормативными и организационно-распорядительными документами университета в области ИБ.

Пользователям запрещено работать под чужими учетными записями, а также сообщать свои пароли и передавать средства аутентификации другим пользователям. При оставлении АРМ пользователями предпринимаются меры по защите их от несанкционированного доступа.

11.3. Контроль доступа к операционной системе

В целях предотвращения несанкционированного доступа к объектам информационной инфраструктуры университета осуществляется контроль доступа к операционной системе (ОС).

Работа пользователей в ОС осуществляется под учетными записями с ограниченными правами. Доступ к ОС предоставляется пользователям только после прохождения процедур идентификации и аутентификации.

Управление учетными записями пользователей, их принадлежностью к группам пользователей, правами и привилегиями, а также политикой парольной защиты осуществляется отделом сетевого и системного администрирования департамента цифрового развития и информатизации.

11.4. Контроль доступа к прикладным системам и информационным активам.

В целях предотвращения несанкционированного доступа к информации и нарушения функционирования информационной инфраструктуры в университете обеспечивается контроль доступа к прикладным системам и информационным активам.

Доступ к прикладным системам и информационным активам предоставляется пользователям после прохождения ими процедур идентификации и аутентификации. При наличии технической возможности целесообразно осуществлять единую аутентификацию в прикладных системах и ОС.

11.5. Контроль доступа к сетевым сервисам.

В целях предотвращения несанкционированного использования сетевых сервисов в информационной инфраструктуре университета осуществляется контроль доступа к сетевым сервисам.

Доступ к сетевым сервисам предоставляется пользователям объектов защиты только в виду служебной необходимости. Порядок разрешения и осуществления доступа пользователей к сетевым сервисам, меры контроля доступа определяются

нормативными и организационно- распорядительными документами университета в области обеспечения ИБ.

11.6. Обеспечение безопасности при удаленном доступе и использовании мобильных устройств.

В целях защиты от несанкционированного доступа в информационную инфраструктуру университета и к защищаемым информационным активам, а также от ее утечки в университете принимаются меры по обеспечению безопасности при осуществлении удаленного доступа и использовании мобильных устройств.

При удаленном подключении пользователей к объектам защиты осуществляется контроль удаленного подключения, включающий применение средств усиленной аутентификации и средств криптографической защиты информационного обмена (защищенных виртуальных сетей).

Перед подключением к информационной инфраструктуре университета все мобильные устройства проверяются на наличие вредоносного ПО и необходимых обновлений системного ПО.

При использовании беспроводных подключений к объектам информационной инфраструктуры университета применяются меры защиты беспроводных сетей.

Меры обеспечения безопасности при использовании мобильных устройств и при осуществлении удаленного доступа определяются нормативными и организационно-распорядительными документами университета в области ИБ.

11.7. Контроль доступа к сетевому оборудованию.

В целях обеспечения безопасности сетевой инфраструктуры университета осуществляется управление доступом администраторов к сетевому оборудованию.

В информационной инфраструктуре университета обеспечивается защита физического и логического доступа к диагностическим и конфигурационным портам сетевого оборудования и сетевых средств защиты. Создается выделенная сеть управления сетевым оборудованием. При осуществлении управления сетевым оборудованием и средствами защиты без использования выделенной сети управления осуществляется криптографическая защита каналов управления.

Доступ к управлению сетевым оборудованием и средствами защиты предоставляется только работникам отдела сетевого и системного администрирования департамента цифрового развития и информатизации.

XII. Обеспечение соответствия требованиям по информационной безопасности

12.1. Обеспечение соответствия правовым требованиям.

В соответствии с законодательством Российской Федерации, требованиями нормативных и организационно-распорядительных документов университета в области ИБ в университете осуществляются меры по защите информации ограниченного доступа.

Защита информации ограниченного доступа в университета обеспечивается организацией:

- защиты персональных данных обучающихся, абитуриентов и работников университета;
- защиты информации, обрабатываемой на объектах информационной инфраструктуры университета;
- защиты информации об архитектуре и конфигурации объектов информационной инфраструктуры университета.

Допускается использование только официально приобретенного лицензионного ПО.

В составе объектов информационной инфраструктуры используются сертифицированные по требованиям безопасности информации или прошедшие оценку соответствия в форме испытаний и приемки средства защиты информации.

Для защиты информации ограниченного доступа криптографическими методами в соответствии с законодательством Российской Федерации, используются сертифицированные по требованиям безопасности информации криптографические средства защиты.

12.2. Организация защиты персональных данных

Перечень мер по защите персональных данных регламентируется Федеральным законом «О персональных данных», локальным нормативным актом университета «Положение о персональных данных», другими организационно- распорядительными документами университета в области ИБ.

12.3. Обеспечение соответствия организационным и техническим требованиям.

В целях предотвращения нарушений ИБ осуществляется контроль выполнения требований нормативных и организационно-распорядительных документов университета в области ИБ.

К числу мер контроля относятся:

- регулярный контроль руководителями структурных подразделений выполнения требований ИБ;
- внутренние проверки департаментом цифрового развития и информатизации соответствия существующих процедур обеспечения ИБ предъявляемым требованиям (внутренний аудит);
- анализ выявленных несоответствий и установление причин их возникновения;
- реализация корректирующих мер и устранение выявленных несоответствий.

12.4. Контроль состояния информационной безопасности.

В целях определения соответствия принимаемых мер безопасности локальным нормативным актам университета по ИБ, выявления угроз ИБ и принятия мер по противодействию им в университете осуществляется контроль состояния ИБ.

Контроль состояния ИБ осуществляется:

- проведением плановых (внеплановых) внешних проверок независимыми организациями и специалистами (внешний аудит);
- проведением внутренних плановых (внеплановых) проверок и постоянным мониторингом, осуществляемыми департаментом цифрового развития и информатизации.

Контроль состояния ИБ осуществляется путем интервьюирования руководителей и работников структурных подразделений, анализа документации, осуществления инструментальных проверок.

Результаты проведения контроля состояния ИБ документируются.

XIII. Ответственность руководителей и работников

13.1. Руководство университета отвечает за состояние ИБ и обеспечивает реализацию настоящей Политики ИБ университета, включая регулярный контроль ее исполнения, актуализацию и выделение необходимых для обеспечения ИБ ресурсов, а также организацию повышения осведомленности и обучения работников в области обеспечения ИБ.

13.2. Работники университета обязаны выполнять следующие общие требования по ИБ:

- соблюдать требования настоящей Политики ИБ и других нормативных и организационно-распорядительных документов университета в области ИБ;
- использовать технические средства обработки информации только в служебных целях;
- осуществлять информирование непосредственного руководителя и департамент цифрового развития и информатизации о выявленных инцидентах ИБ.

13.3. Работникам университета запрещается нарушать установленные правила обеспечения ИБ и скрывать факты возникновения инцидентов ИБ.

13.4. Работники университета, не выполняющие требования настоящей Политики ИБ или требования нормативных и организационно-распорядительных документов университета в области ИБ, могут быть привлечены к ответственности установленным порядком.

XIV. Порядок пересмотра политики и история изменений

14.1. Политика ИБ университета пересматривается с периодичностью не реже чем 1 раз в 3 года. При пересмотре Политики ИБ университета учитываются результаты контроля эффективности обеспечения ИБ за предыдущий период.

Процедура пересмотра Политики ИБ университета включает:

- анализ и выявление несоответствий действующей Политики ИБ университета текущим условиям;
- разработку предложений по совершенствованию Политики ИБ университета;
- утверждение новой редакции Политики ИБ университета.

При осуществлении процедуры пересмотра учитываются:

- результаты контроля состояния ИБ и предложения структурных подразделений о совершенствовании процедур обеспечения ИБ;
- изменения в организационно-штатной структуре университета и в его информационной инфраструктуре;
- изменения в законодательной и нормативной базе по ИБ, произошедшие с момента утверждения предыдущей Политики ИБ университета;
- результаты анализа произошедших инцидентов ИБ, а также уязвимости и угрозы, выявленные в университете за время, прошедшее с момента утверждения предыдущей Политики ИБ университета;
- изменения в управлении ИБ, включая изменения в распределении ресурсов и обязанностей при обеспечении ИБ.

14.2. Все вносимые в политику ИБ изменения подлежат регистрации. Измененной Политике ИБ разработчик присваивает следующий по порядку номер версии.

История изменений

Дата	Версия	Описание изменений	Автор
10.06.2006	1.0	Первоначальная редакция.	ЦТО
12.11.2008	2.0	Изменения организационной структуры системы информационной безопасности. Изменения, связанные с разработкой и принятием Политики антивирусной защиты, Политики управления доступом и Плана обеспечения непрерывной работы и восстановления работоспособности информационных систем.	ЦТО
01.02.2011	3.0	Изменения в наименовании подразделений. Корректировка перечня информационных систем.	Управление информатизации
12.09.2014	4.0	Изменения организационно-штатной структуры Университета и системы управления информационной безопасностью	Управление информатизации
10.12.2019	5.0	Изменения организационно-штатной структуры Университета и системы управления информационной безопасностью	Управление информатизации
2_.05.2023	6.0	Изменения организационно-штатной структуры Университета и системы управления информационной безопасностью	Департамент цифрового развития и информатизации

Приложение 1

к политике информационной безопасности

Обязательство работника ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» о соблюдении режима конфиденциальности персональных данных

Я _____
(фамилия имя отчество)

_____
(должность)

проживающая (ий) по адресу _____

паспорт_____выдан_____,

в период трудовых (служебных) отношений с ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» (198035, г. Санкт-Петербург, ул. Двинская, д. 5/7) и в течение 3 лет после их окончания обязуюсь:

1. Не разглашать, не передавать третьим лицам и не раскрывать публично сведения, составляющие персональные данные работников и/или обучающихся, которые мне будут доверены или станут известны в связи с исполнением служебных обязанностей.
2. Выполнять, относящиеся ко мне требования, предусмотренные приказами, распоряжениями, инструкциями и другими локальными нормативными актами по обеспечению режима конфиденциальности персональных данных работников и обучающихся и соблюдению правил их обработки.
3. В случае попытки посторонних лиц получить от меня сведения, составляющие персональные данные работников и/или обучающихся, немедленно сообщить об этом своему непосредственному начальнику или уполномоченному лицу по обеспечению безопасности персональных данных в информационных системах (начальнику управления информатизации).
4. При увольнении все носители, содержащие персональные данные работников и/или обучающихся (зарегистрированные документы, черновики, магнитные и магнитно-оптические носители информации и др.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей, передать руководителю своего структурного подразделения.
5. Об утрате или недостаче документов или иных носителей, содержащих персональные данные работников и/или обучающихся, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению персональных данных работников и/или обучающихся, а также о причинах и условиях возможной утечки сведений немедленно сообщать уполномоченному лицу по обеспечению безопасности персональных данных в информационных системах (начальнику управления информатизации).

Мне известно, что нарушение этих требований может повлечь уголовную, административную, гражданско-правовую или иную ответственность в соответствии законодательством РФ, в виде лишения свободы, денежного штрафа, обязанности по возмещению ущерба ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» и других наказаний.

Мне известно, что принимаемое мною Обязательство является неотъемлемой частью моего Трудового договора и станет юридическим основанием для привлечения меня к ответственности в случае нарушения мною положений настоящего Обязательства.

Подпись заверяю:

_____/_____/ _____/_____/

"___"_____202__г. м.п.