МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Ректор
_____ В.Д. Нечаев
«18» 03 2025 г.
№24-02-01-09/158

к приказу
от 18.03.2025 № 563-п

ПОЛОЖЕНИЕ
об ответственном за обеспечение информационной безопасности Азовского морского института (Мариупольского филиала федерального государственного автономного образовательного учреждения высшего образования «Севастопольский государственный университет» в Донецкой Народной Республике)

г. Севастополь

Содержание

1. Общие положения

1.1. Настоящее Положение определяет полномочия, права и обязанности ответственного лица за обеспечение информационной безопасности, в том числе за обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и реагирование на компьютерные инциденты в Азовском морском институте (Мариупольского филиала федерального государственного автономного образовательного учреждения высшего образования «Севастопольский государственный университет» (далее – Университет) в Донецкой Народной Республике) (далее – Филиал).

1.2. Настоящее Положение разработано с учетом требований Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Постановления Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».

1.3. Ответственное лицо определяется и назначается приказом ректора Университета.

1.4. Ответственное лицо осуществляет свою деятельность на основе должностной инструкции и подчиняется непосредственно ректору Университета.

1.5. Ответственное лицо входит в состав коллегиальных органов Университета.

1.6. Указания и поручения ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми работниками Филиала.

2. Квалификационные требования к ответственному лицу

2.1. Ответственное лицо должно иметь высшее образование (не ниже уровня специалитета, магистратуры) по направлению обеспечения информационной безопасности. Если ответственное лицо имеет высшее образование по другому направлению подготовки (специальности), он должен пройти обучение по программе профессиональной переподготовки по направлению «Информационная безопасность».

2.2. Для ответственного лица требуются наличие следующих знаний, умений и профессиональных компетенций:

2.2.1. основные (в том числе бизнес и управленческие) процессы Филиала и специфика обеспечения информационной безопасности Филиала;

2.2.2. влияние информационных технологий на деятельность Филиала, в

том числе:

– роль и место информационных технологий (степень интеграции информационных технологий) в процессах функционирования Филиала;

– зависимость основных процессов функционирования Филиала от информационных технологий;

2.2.3. информационно-телекоммуникационные технологии, в том числе:

– современные информационно-телекоммуникационные технологии, используемые в Филиале;

– способы построения информационных систем, информационно-телекоммуникационных сетей (далее – системы и сети), в том числе ограниченного доступа;

– типовые архитектуры систем и сетей, требования к их оснащенности программными (программно-техническими) средствами;

– принципы построения и функционирования современных операционных систем, систем управления базами данных, систем и сетей, основных протоколов систем и сетей;

2.2.4. обеспечение информационной безопасности, в том числе:

– цели, задачи, основы организации, ключевые элементы, основные способы и средства обеспечения информационной безопасности;

– цели обеспечения информационной безопасности применительно к основным процессам функционирования Филиала и Университета, реализации и контроля их достижения;

– принципы и направления стратегического развития информационной безопасности в Филиале;

– правила разработки, утверждения и отмены организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Филиале, состав и содержание таких документов;

– порядок организации работ по обеспечению информационной безопасности в Филиале;

– основные негативные последствия, наступление которых возможно в результате реализации угроз безопасности информации, способы и методы обеспечения и поддержания необходимого уровня (состояния) информационной безопасности Филиала для исключения (невозможности реализации) негативных последствий, а также порядок проведения практических проверок и контроля результативности применяемых способов и методов обеспечения информационной безопасности в Филиале;

– основные угрозы безопасности информации, предпосылки их возникновения и возможные пути их реализации, а также порядок оценки таких угроз;

– возможности и назначения типовых программных, программно-аппаратных (технических) средств обеспечения информационной безопасности;

– способы и средства проведения компьютерных атак, актуальные тактики и техники нарушителей;

– порядок организации взаимодействия структурных подразделений Филиала при решении вопросов обеспечения информационной безопасности;

– управление проектами по информационной безопасности;

– антикризисное управление и принятие управленческих решений при реагировании на кризисы и компьютерные инциденты;

– планирование деятельности по обеспечению информационной безопасности в Филиале;

– формулирование измеримых и практических результатов деятельности по обеспечению информационной безопасности Филиала;

– организация разработки политики (правил, процедур), регламентирующей вопросы информационной безопасности;

– внедрение политики;

– организация контроля и анализа применения политики;

– организация мероприятий по разработке единых инструментов и механизмов контроля деятельности по обеспечению информационной безопасности в Филиале;

– поддержка и совершенствование деятельности по обеспечению информационной безопасности в Филиале;

– организация мероприятий по определению угроз безопасности информации систем и сетей, а также по формированию требований к обеспечению информационной безопасности в Филиале;

– организация внедрения способов и средств для обеспечения информационной безопасности в Филиале;

– организация мероприятий по анализу и контролю состояния информационной безопасности Филиала и модернизации (трансформации) процессов функционирования Филиала в целях обеспечения информационной безопасности;

– обеспечение информационной безопасности в ходе эксплуатации систем и сетей, а также при выводе их из эксплуатации;

– организация мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Филиала и реагированию на компьютерные инциденты;

– организация мероприятий по отслеживанию и контролю достижения целей информационной безопасности (фактически достигнутый эффект и результат) в Филиале.

2.3. С учетом области и вида деятельности Филиала от ответственного лица требуется знание нормативных правовых актов Российской Федерации, методических документов, международных и национальных стандартов в области:

– защиты государственной тайны;

– защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных;

– обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

– обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

– создания и обеспечения безопасного функционирования государственных информационных систем и информационных систем в защищенном исполнении;

– создания, обеспечения технических условий установки и эксплуатации средств защиты информации;

– иных нормативных правовых актов и стандартов в области информационной безопасности.

3. Трудовые (должностные) обязанности ответственного лица

3.1. Ответственное лицо принимает участие в формировании политики Филиала, отвечает за согласование стратегии развития Филиала в части вопросов обеспечения информационной безопасности.

3.2. Ответственное лицо:

– организует разработку политики, направленной в том числе на обеспечение и поддержание стабильной деятельности Филиала и его процессов функционирования в случае проведения компьютерных атак, отвечает за согласование и утверждение политики в Филиале, реализацию мероприятий, предусмотренных политикой, отслеживает и контролирует результаты реализации политики;

– организует работу по обеспечению информационной безопасности Филиала, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты, формулированию перечня негативных последствий, проведению мероприятий по их недопущению, отслеживанию и контролю эффективности (результативности) таких мероприятий, а также по необходимому информационному обмену;

– организует реализацию и контроль проведения в Филиале организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации (далее – ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) с учетом меняющихся угроз в информационной сфере, а также самостоятельно ответственным лицом в результате своей деятельности;

Дирекция правового обеспечения и внутреннего контроля
И.С. Магера

– организует беспрепятственный доступ (в том числе удаленный) должностным лицам ФСБ России и ее территориальных органов к информационным ресурсам, принадлежащим Филиалу либо используемым Филиалом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет», в целях осуществления мониторинга их защищенности, а также работникам структурного подразделения, осуществляющего функции по обеспечению информационной безопасности;

– организует взаимодействие с должностными лицами ФСБ России и ее территориальных органов, в том числе контроль исполнения указаний, данных ФСБ России и ее территориальными органами по результатам мониторинга защищенности информационных ресурсов, принадлежащих Филиалу либо используемых Филиалом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

– организует контроль за выполнением требований нормативных правовых актов, нормативно-технической документации, за соблюдением установленного порядка выполнения работ при решении вопросов, касающихся защиты информации;

– организует развитие информационной безопасности, формирование и развитие навыков работников Филиала в сфере информационной безопасности;

– организует разработку и реализацию мероприятий по обеспечению информационной безопасности в Филиале в соответствии с требованиями к обеспечению информационной безопасности, установленными федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации;

– организует контроль пользователей информационных ресурсов Филиала в части соблюдения ими режима конфиденциальности информации, правил работы со съемными машинными носителями информации, выполнения организационных и технических мер по защите информации;

– организует планирование мероприятий по обеспечению информационной безопасности в Филиале;

– организует подготовку правовых актов, иных организационно-распорядительных документов по вопросам обеспечения информационной безопасности в Филиале, осуществляет согласование иных документов Филиала в части обеспечения информационной безопасности;

– организует проведение научно-исследовательских и опытно-конструкторских работ по вопросам обеспечения информационной безопасности в Филиале;

– организует проведение контроля за состоянием обеспечения информационной безопасности в Филиале, включая оценку защищенности

систем и сетей Филиала.

3.3. Ответственное лицо:

– осуществляет регулярный контроль текущего уровня (состояния) информационной безопасности в Филиале, а также отвечает за реализацию мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности в Филиале, в том числе с учетом появления новых угроз безопасности информации и современных способов и методов проведения компьютерных атак;

– осуществляет регулярное и своевременное информирование ректора Университета (уполномоченное им лицо) о компьютерных инцидентах, текущем уровне (состоянии) информационной безопасности и результатах практических учений по противодействию компьютерным атакам;

– осуществляет контроль за ведением организационно-распорядительной документации, статистического учета и отчетности по курируемым разделам работы;

– осуществляет согласование требований к системам и сетям Филиала в части обеспечения информационной безопасности;

– осуществляет руководство структурным подразделением Филиала, обеспечивающим информационную безопасность.

3.4. Ответственное лицо:

– организует и контролирует проведение мероприятий по анализу и оценке состояния информационной безопасности Филиала и контролирует их результаты;

– организует и контролирует функционирование системы обеспечения информационной безопасности в Филиале;

– координирует деятельность иных структурных подразделений Филиала по вопросам обеспечения информационной безопасности.

3.5. Ответственное лицо согласовывает политику, технические задания и иную основополагающую документацию в сфере информационных технологий, цифровизации и цифровой трансформации в Филиале.

3.6. Ответственное лицо с использованием нормативных правовых документов и методических материалов ФСБ России организует обнаружение, предупреждение и ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты с информационными ресурсами Филиала, а также взаимодействие с Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ) одним (или несколькими) из следующих способов:

– силами структурного подразделения, ответственного за обеспечение информационной безопасности, с заключением соглашения (издания совместного акта) о взаимодействии с ФСБ России (НКЦКИ), включающего в том числе права и обязанности сторон, порядок проведения

совместных мероприятий, регламент информационного обмена, порядок и сроки представления отчетности, порядок и формы контроля;

– силами структурного подразделения, ответственного за обеспечение информационной безопасности, с его аккредитацией как центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА);

– силами организаций, являющихся аккредитованными центрами ГосСОПКА.

3.7. Ответственное лицо обеспечивает планирование и реализацию мероприятий по переводу систем и сетей на отечественные средства защиты информации, а также контроль за соблюдением запрета на использование средств защиты информации, странами происхождения которых являются иностранные государства в соответствии с пунктом 6 Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

3.8. Ответственное лицо сопровождает мероприятия по разработке (модернизации) систем и сетей в части информационной безопасности, а также требований нормативных правовых актов, нормативно-технических и методических документов по защите информации и выполнения этих требований.

3.9. Ответственное лицо проводит работу по унификации способов и средств по обеспечению информационной безопасности, иных технических решений в Филиале.

3.10. Ответственное лицо принимает меры по совершенствованию обеспечения информационной безопасности в Филиале.

3.11. Ответственное лицо повышает на постоянной основе профессиональную компетенцию, знания и навыки в области обеспечения информационной безопасности.

3.12. Ответственное лицо выполняет иные обязанности, исходя из возложенных полномочий и поставленных ректором Университета (уполномоченного им лица) задач в рамках обеспечения информационной безопасности Филиала.

3.13. Ответственное лицо:

– соблюдает и обеспечивает выполнение законодательства Российской Федерации;

– в случаях, установленных законодательством Российской Федерации, согласовывает политику с ФСБ России и ФСТЭК России;

– представляет по запросам ФСБ России и ФСТЭК России достоверные сведения о результатах реализации политики (фактически достигнутом эффекте и результате) и текущем уровне (состоянии) информационной безопасности в Филиале;

– поддерживает уровень квалификации и постоянно развивает свои навыки в области информационной безопасности, необходимые для обеспечения информационной безопасности в Филиале;

– организовывает при необходимости проведение и участвует в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

– участвует в пределах компетенции в осуществлении закупок товаров, работ, услуг для обеспечения нужд в сфере информационной безопасности.

4. Права ответственного лица

4.1. Ответственное лицо имеет право:

– давать указания и поручения Филиала в части обеспечения информационной безопасности;

– запрашивать от работников Филиала информацию и материалы, необходимые для реализации возложенных на ответственное лицо прав и обязанностей;

– участвовать в заседаниях (совещаниях) коллегиальных органов Филиала, принятии решений по вопросам деятельности Филиала, а также по внесению предложений по совершенствованию деятельности Филиала;

– участвовать в разработке политики;

– представлять результаты реализации политики коллегиальному органу Университета;

– принимать решения по вопросам обеспечения информационной безопасности Филиала;

– взаимодействовать с ФСБ России, ФСТЭК России и иными федеральными органами исполнительной власти по вопросам обеспечения информационной безопасности, в том числе по вопросам совершенствования законодательства Российской Федерации в области обеспечения информационной безопасности;

– вносить предложения о привлечении организаций, имеющих соответствующие лицензии на деятельность в области защиты информации, в соответствии с законодательством Российской Федерации к проведению работ по обеспечению информационной безопасности;

– инициировать проверки уровня (состояния) обеспечения информационной безопасности в Филиале;

– организовывать на объектах Филиала мероприятия по информационной безопасности, разработку и представление ректору Университета (уполномоченному им лицу) предложений по внесению

изменений в процессы функционирования, принятию других мер, направленных на недопущение реализации негативных последствий;

– получать доступ в установленном порядке к сведениям, составляющим государственную тайну, если исполнение обязанностей ответственного лица связано с использованием таких сведений и наличием необходимых прав и полномочий;

– получать доступ в установленном порядке в связи с исполнением своих обязанностей в государственные органы, органы местного самоуправления, общественные объединения и другие организации;

– обеспечивать надлежащие организационно-технические условия, необходимые для исполнения обязанностей ответственного лица.

5. Ответственность ответственного лица

5.1. Ответственное лицо в соответствии с законодательством Российской Федерации несет ответственность:

– за неисполнение или ненадлежащее исполнение своих обязанностей;

– за действия (бездействие), ведущие к нарушению прав и законных интересов Филиала;

– за разглашение государственной тайны и иных сведений, ставших ему известными в связи с исполнением своих обязанностей;

– за достижение целей обеспечения информационной безопасности;

– за поддержание и непрерывное развитие информационной безопасности Филиала для исключения (невозможности реализации) негативных последствий;

– за организацию мероприятий по разработке (модернизации) систем и сетей в части информационной безопасности Филиала;

– за нарушения требований по обеспечению информационной безопасности;

– за нарушения в обеспечении защиты систем и сетей, повлекшие негативные последствия.

6. Заключительные положения

6.1. Настоящее Положение вступает в силу с момента его утверждения приказом ректора Университета.

6.2. Внесение изменений и дополнений в настоящее Положение осуществляется путем подготовки изменений, дополнений или принятием Положения в новой редакции.

6.3. Изменения или дополнения к настоящему Положению, Положение в новой редакции утверждаются приказом ректора.

Дирекция правового обеспечения и внутреннего контроля
И.С. Магера

6.4. Настоящее Положение подлежит регистрации в составе документов организационного характера номенклатуры дел Отдела делопроизводства и архивного обеспечения.

6.5. Подлинный экземпляр настоящего Положения подлежит хранению в составе документов организационного характера в Отделе делопроизводства и архивного обеспечения до замены его Положением в новой редакции.