Федеральное агентство морского и речного транспорта

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

Положение по мониторингу информационной безопасности и контролю защитных мер

Санкт-Петербург
2023

СТРАНИЦА СТАТУСА ДОКУМЕНТА

Приложение № 4

к приказу ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»
от 29.05.2023 № 601

Система менеджмента качества **Положение по мониторингу информационной безопасности и контролю защитных мер**	Новая редакция
	Дата введения - в соответствии с приказом

Настоящее Положение по мониторингу информационной безопасности и контролю защитных мер разработано согласно требованиям Международного Стандарта ISO 9001:2015 и является документом системы менеджмента качества ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова». Положение по мониторингу информационной безопасности и контролю защитных мер разработано в соответствии с действующим законодательством и нормативными правовыми актами Российской Федерации. Настоящее Положение является общедоступным документом, дополняющим политику информационной безопасности ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» в части осуществления мероприятий и процедур, направленных на снижение потенциального ущерба от реализации угроз информационной безопасности до приемлемого уровня.

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

Лист учета экземпляров

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

Место хранения некорректируемого экземпляра	№ экземпляра
Общй отдел	1
Корпоративный портал	3

Лист учета корректуры

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

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Ведение контрольных журналов – фиксирование данных о событиях, связанных с информационной безопасностью, в целях проверки, анализа и постоянного мониторинга.

Информационная безопасность (ИБ) – состояние защищенности интересов университета в условиях угроз в информационной сфере.

Примечание.

Защищенность достигается обеспечением совокупности свойств ИБ – доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) университета.

Защитная мера – сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ университета.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для университета; находящаяся в распоряжении университета и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Информационная инфраструктура – совокупность сетей передачи данных, серверов, системного и прикладного программного обеспечения, информационных систем, персональных компьютеров, средств защиты

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.

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.

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

Мониторинг информационной безопасности – процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей.

Данные мониторинга – данные о состоянии объектов мониторинга ИБ, а также данные, получаемые из среды функционирования объектов мониторинга и внешних сервисов, которые могут использоваться для выявления уязвимостей и угроз безопасности информации.

Источники данных мониторинга – программные или программно-технические средства, с которых может быть осуществлен сбор данных мониторинга.

Объект доступа – объект информатизации, представляющий собой аппаратное средство, средство вычислительной техники и (или) сетевое оборудование, в том числе входящее в состав ИС университета.

Объект мониторинга – объект или процесс, изменение состояния которого может привести к нарушению безопасности информации.

Рабочая станция – ЭВМ, подключаемая к информационно-вычислительной сети, имеющая потенциальную возможность выхода в сеть Интернет, имеющая все приложения Microsoft Office, способная осуществлять доступ к корпоративным информационным ресурсам и прикладным информационным системам, обеспеченная централизованной антивирусной защитой.

Система информационной безопасности – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и организационное обеспечение, необходимое для применения указанных защитных мер.

Сетевое администрирование – повседневная эксплуатация и управление сетевыми процессами и средствами, используемыми сетью.

Сетевой мониторинг – процесс постоянного наблюдения и проверки зафиксированных данных о сетевой деятельности и операциях, включая контрольные журналы и предупреждения об опасности, и связанный с этим анализ.

Событие (информационной) безопасности – зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой средств ЗИ, или ситуацию, которая может быть значимой для безопасности информации.

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Удаленный доступ – процесс получения доступа к сетевым ресурсам из другой сети или с терминала, не являющегося постоянно соединенным физически или логически с сетью, к которой он получает доступ.

Ущерб – утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры университета или другой вред активам и (или) инфраструктуре университета, наступивший в результате реализации угроз информационной безопасности через уязвимости информационной безопасности.

Уязвимость – свойство информационной (автоматизированной) системы, обуславливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

Физический доступ к объекту доступа – доступ к объекту доступа, включая доступ в помещения, в котором расположен объект доступа, позволяющий осуществить физическое воздействие на него.

Фильтрация событий безопасности – выборка данных о событиях безопасности информации из состава данных, передаваемых для дальнейшего мониторинга ИБ или долгосрочного хранения по определенным критериям (правилам) мониторинга ИБ.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС – автоматизированная система
АРМ – автоматизированное рабочее место
ДЦРИ – департамент цифрового развития и информатизации
ИБ – информационная безопасность
ИСПДн – информационная система персональных данных
ИС – информационная система
НСД – несанкционированный доступ
НРД — нерегламентированные действия в рамках предоставленных полномочий
СКЗИ – средство криптографической защиты информации
СКС – структурированная кабельная система
ЭВМ – электронная вычислительная машина
ЭЦП – электронная цифровая подпись
ПО – программное обеспечение
СУБД – системы управления базами данных
ОССА – отдел защиты информации и администрирования
ОС – операционная система
БД – база данных
СВТ – средство вычислительной техники
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
университет – ГУМРФ имени адмирала С.О. Макарова

1. ОБЩИЕ ТРЕБОВАНИЯ

1.1. Настоящее Положение по мониторингу информационной безопасности и контролю защитных мер (далее – Положение) устанавливает требования к процедурам проведения мониторинга системы обеспечения информационной безопасности информационной инфраструктуры университета, порядок контроля защитных мер, направленных на защиту информационных активов от различных угроз ИБ, а также ответственность и контроль их выполнения.

1.2. Документ разработан на основе внутренних нормативных документов университета, Политики информационной безопасности университета.

1.3. Настоящее Положение распространяется на работников департамента цифрового развития и информатизации и других работников структурных подразделений университета (включая представителей внешних организаций), принимающих участие в тестировании, эксплуатации, сопровождении и (или) обеспечении информационной безопасности АС, входящих в состав информационной инфраструктуры университета.

1.4. Настоящее Положение дополняет Политику информационной безопасности Университета в части осуществления мероприятий и процедур, направленных на снижение потенциального ущерба от реализации угроз ИБ до приемлемого уровня.

1.5. В настоящем Положении не рассматриваются вопросы, связанные с мониторингом и менеджментом инцидентов ИБ университета. Данные вопросы должны быть изложены в частной политике по менеджменту инцидентов ИБ.

1.6. Вопросы, связанные с проверками и оценкой ИБ университета путем проведения самооценок ИБ и аудита ИБ изложены в Положении по организации внутреннего контроля соответствия обработки персональных данных и в настоящем Положении не рассматриваются.

1.7. Функции по организации проведения мониторинга ИБ университета, а также контроля защитных мер возлагаются на работников отдела сетевого и системного администрирования департамента цифрового развития и информатизации (далее – ОССА ДЦРИ) в соответствии с должностными инструкциями. В своей работе ОССА ДЦРИ руководствуются положением об ОССА, содержащем разъяснения в части выполняемых функций.

2. ПОРЯДОК ПРОВЕДЕНИЯ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Мониторинг информационной безопасности университета включает в себя мероприятия как организационного, так и технического уровня, которые проводятся на регулярной и постоянной основе. Мониторинг ИБ рассматривается как процесс регулярного наблюдения за событиями ИБ в информационной инфраструктуре университета с целью своевременного выявления и реагирования на действия, которые привели или могут привести к реализации угроз ИБ.

2.2. Основными целями мониторинга и контроля защитных мер в университете являются:

- контроль реализации положений внутренних документов университета, регламентирующих вопросы обеспечения ИБ;
- выявление нештатных, в том числе злоумышленных, действий в рамках информационной инфраструктуры университета;
- выявление инцидентов ИБ.

Мониторинг и контроль защитных мер проводится работниками ОССА ДЦРИ.

2.3. Мониторинг событий и инцидентов ИБ используется в качестве оперативной меры для поддержания системы защиты на должном уровне. Менеджмент событий и инцидентов безопасности, полученных в результате мониторинга, позволяет избежать деградации и обеспечить требуемый уровень безопасности активов.

2.4. Департаментом цифрового развития и информатизации определяются процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции. При проведении процедур мониторинга и анализа данных регистрации, действий и операций используются специализированные программные и (или) технические средства. Для осуществления мониторинга и контроля за компонентами информационной инфраструктуры университета, включающими в себя серверы приложений, базы данных и прочие сетевые устройства и серверы, а также рабочие станции управления сетью, выделяется подсистема автоматизированного мониторинга и контроля ИБ, в которую данные средства интегрируются.

2.5. Процедуры в части мониторинга ИБ университета определяются в рамках следующих областей:

- защиты научных и учебно-образовательных процессов, в рамках которых обрабатываются персональные данные;
- использования технических средств АС в части информационной безопасности;
- использования электронной почты и ресурсов сети Интернет;
- протоколирования событий и системного аудита;
- защиты от НСД и НРД, управления доступом и регистрации пользователей в части информационной безопасности;
- антивирусной защиты;
- использования СКЗИ.

2.5.1. Мониторинг научных и образовательных процессов осуществляется в виде:

- контроля состояния рабочих мест, на которых производится обработка, передача и хранение информации;
- контроля протоколов работы средств защиты от вредоносного ПО;
- контроля протоколов работы ПО, обеспечивающего доступ пользователей к корпоративной электронной почте и сети Интернет;
- контроля действий и доступа пользователей к информационным ресурсам с использованием средств аудита сетевых операционных систем, средств СУБД, АРМ.

2.5.2. Мониторинг использования технических средств и компонент информационной инфраструктуры университета в части информационной безопасности осуществляется в виде:

- проверок работоспособности программно-технических компонент АС, входящих в состав информационной инфраструктуры университета, в процессе их администрирования и при проведении работ по техническому обслуживанию;
- проверок наиболее существенных компонент информационной инфраструктуры университета посредством встроенных средств и механизмов контроля работоспособности – в рамках работы администраторов соответствующих систем;
- проверок по выявлению попыток НСД и НРД и других событий, связанных с неправомерными или подозрительными операциями.

2.5.3 Мониторинг использования электронной почты и ресурсов сети Интернет осуществляется в виде:

- выявление отправки/получения писем электронной почты с несанкционированным или опасным содержимым;
- проверок по выявлению попыток нарушения существующих правил и политик по использованию электронной почты и сети Интернет.

2.5.3. Мониторинг в рамках защиты от НСД и НРД, мониторинг управления доступом и регистрации пользователей в части информационной безопасности осуществляется в виде:

- отслеживания событий, влияющих на безопасность информационной инфраструктуры университета;
- регистрации событий (например, неудачных попыток входа в систему), связанных с безопасностью, в журналах автоматизированного мониторинга и контроля;
- выявления нарушений безопасности путем анализа данных журналов мониторинга в ручном режиме с использованием встроенных программных средств.

2.5.4. Средства протоколирования (автоматизированного мониторинга и контроля) должны применяться на всех рубежах защиты в следующем объеме:

На рубеже защиты внешнего периметра протоколируются следующие события:

- информация о состоянии внешнего маршрутизатора, МЭ, прокси-сервера, сервера удаленного доступа, модемов, межсетевых экранов уровня приложений и иных пограничных устройств;
- доступ внешних пользователей к внутренним информационным ресурсам;
- доступ внутренних пользователей к внешним информационным ресурсам.

На рубеже сетевой инфраструктуры осуществляется протоколирование информации о состоянии кабельной сети и активного сетевого оборудования, а также структуры информационного обмена на сетевом и транспортном уровнях.

На рубеже защиты серверов и рабочих станций средствами автоматизированного мониторинга и контроля ОС обеспечивается протоколирование всех системных событий, связанных с безопасностью, включая удачные и неудачные попытки регистрации пользователей в системе, доступ к системным ресурсам, изменение политики мониторинга и контроля и т. п.

На уровне приложений средствами данных приложений обеспечивается регистрация событий, связанных с их функционированием.

Подсистема мониторинга предусматривает возможность регистрации следующих событий:

- разрешения на выполнение запрошенных операций;
- запрещение выполнения запрошенных операций;
- удачные и неудачные попытки изменения атрибутов безопасности;
- удачные и неудачные попытки доступа к аутентификационной информации пользователей;
- попытки использования функций управления атрибутами безопасности пользователей;
- любое использование механизмов идентификации и аутентификации;
- использование функций администрирования, связанных с безопасностью;
- запросы на получение административных полномочий;
- блокирование и разблокирование пользовательских сессий;
- инициирование и завершение пользовательских сессий;
- запуск и остановка процессов;
- удачные и неудачные попытки доступа к критичным системным файлам.

Каждая запись мониторинга и контроля должна содержать как минимум следующие данные:

- дату и время события, тип события, идентификаторы субъекта и объекта доступа, результат события (успешное или неуспешное);
- другая специфичная для определенного вида событий информация – на уровне, необходимом для предотвращения и расследования инцидентов ИБ.

Все события мониторинга ассоциируются с пользователями, инициировавшими эти события.

В части парольной защиты и контроля надежности пользовательских паролей мониторинг предусматривает применение средств анализа защищенности с целью выявления слабых паролей.

2.5.5. Мониторинг использования СКЗИ осуществляется в виде:

- контроля всех значимых событий, состоявшихся в процессе обмена криптографически защищенными данными, и всех инцидентов ИБ на основе протоколов работы СКЗИ;
- периодических проверок состояния технической и эксплуатационной документации на СКЗИ;
- периодических проверок журналов учета СКЗИ, эксплуатационной и технической документации к ним в подразделениях университета, использующих СКЗИ;
- проверок ведения журналов учета лиц, допущенных к работе с СКЗИ;
- проверок технического состояния СКЗИ, а также проверок соблюдения в подразделениях университета правил пользования СКЗИ и порядка обращения с ключевыми документами к ним;
- проверки выполнения требований по размещению, специальному оборудованию, охране и организации режима в помещениях, где установлены СКЗИ или хранятся ключевые документы, а также проверки соответствия режима хранения СКЗИ и ключевой документации предъявляемым требованиям;
- проверки разбирательств и составления заключений по фактам нарушения условий использования СКЗИ;
- проверки выполнения других требований, изложенных в Инструкции по обращению со средствами криптографической защиты информации и инструкции ответственного за организацию работ по криптографической защите информации.

2.5.6. Антивирусный мониторинг осуществляется в виде:

- контроля установки, настройки и сопровождения средств защиты, в том числе проверок правильности настройки средств защиты, своевременности обновления средств защиты, сигнатурных баз на рабочих станциях и серверах на соответствие руководствам;
- проведения антивирусного контроля в подразделениях университета, а также других требований, предусмотренных данным Положением.

2.5.7. Системный аудит.

Для анализа защищенности и проведения последующих проверок компонент информационной инфраструктуры университета используются средства системного и прикладного уровней, предназначенные для решения следующих основных задач:

- анализ параметров конфигурации операционных систем и приложений по шаблонам с целью выявления уязвимостей, связанных с их некорректной настройкой, определения уровня защищенности контролируемых систем и уровня соответствия политике информационной безопасности университета;
- контроль и анализ установленных обновлений информационной безопасности.

Для проведения процедур системного аудита университет использует специализированное ПО, одной из функций которого является проведение инвентаризации программного и аппаратного обеспечения.

Обнаружение уязвимостей осуществляется путем сравнения эталонных значений с текущими параметрами настройки ОС и приложений.

Контроль изменения состояний контролируемых систем осуществляется путем сравнения их текущего состояния с мгновенными снимками, сделанными в ходе осуществления предыдущих проверок.

Контроль целостности файлов производится по контрольным суммам.

Уровень защищенности контролируемой системы определяется в зависимости от количества обнаруженных уязвимостей и степени их критичности.

Выявление уязвимостей системы защиты информации университета производится ежегодно.

Актуализация базы данных уязвимостей осуществляется ежемесячно (должны обнаруживаться все известные уязвимости, информация о которых имеется на специализированных Web-серверах Интернет).

Целью выполнения процедур системного аудита является обнаружение следующих видов уязвимостей:

- уязвимости операционных систем, включая системные и сетевые сервисы, входящие в их состав;
- уязвимости СУБД, Web, файловых и почтовых серверов;
- уязвимости МЭ;
- слабые пароли пользователей (выявляются путем проверки политики выработки паролей);
- подверженность системы атакам на отказ в обслуживании;
- неустановленные пакеты программных коррекций;
- уязвимости системного реестра Windows;
- уязвимости конфигурационных файлов операционных систем;
- уязвимости пользовательских регистрационных записей.

Программные средства мониторинга не должны выполнять атаки на отказ в обслуживании и иные действия, негативно влияющие на производительность функционирующих систем, но должны обнаруживать соответствующие уязвимости.

2.6. Процедуры мониторинга ИБ и контроля защитных мер регулярно пересматриваются в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ. Результаты пересмотра документально фиксируются.

Порядок пересмотра процедур мониторинга ИБ и контроля защитных мер определяется настоящим Положением.

3. КОНТРОЛЬ СОБЛЮДЕНИЯ ЗАЩИТНЫХ МЕР

3.1. Контроль защитных мер, направленных на минимизацию рисков, присущих научным и образовательным процессам (далее – контроль), является неотъемлемой частью общего комплекса мер обеспечения безопасности и защиты информации в университете.

3.2. Контроль соблюдения защитных мер осуществляется на всех этапах обработки информации как для информационной инфраструктуры университета в целом, так и для отдельных научных и образовательных процессов.

3.3. Контроль соблюдения защитных мер осуществляется на всех стадиях жизненного цикла автоматизированных/информационных систем (разработка технических заданий, проектирование, создание и тестирование, приемка и ввод в действие, эксплуатация, сопровождение и модернизация, снятие с эксплуатации).

3.4. Выделяется внутренний и внешний контроль.

3.4.1. Внешний контроль осуществляется в рамках следующих контрольных мероприятий:

- контроль и надзор за выполнением требований по обеспечению безопасности персональных данных при их обработке в ИСПДн, осуществляемый ФСТЭК России и ФСБ России в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИСПДн.

3.4.2. Внутренний контроль осуществляется в рамках следующих контрольных мероприятий:

- приемочные испытания АС/ИС (после разработки или модификации АС/ИС);

- мониторинг и контроль защитных мер;
- периодические комплексные, тематические (целевые), контрольные проверки, проводимые департаментом цифрового развития и информатизации;
- проверки, проводимые в рамках реализации системы менеджмента качества;
- самооценки соответствия информационной безопасности требованиям Росморречфлота и Минобрнауки России.

Все указанные контрольные мероприятия (внешние и внутренние) обеспечивают распределенный во времени процесс подтверждения соответствия АС/ИС университета требованиям по обеспечению информационной безопасности.

3.5. Контроль информационной безопасности процесса (объекта) включает следующие составляющие:

- документирование процесса (технологии, конфигурации объекта);
- выявление контрольных точек процесса (объекта) – операций, действий, состояний, в наибольшей степени влияющих на уровень безопасности процесса или его результата;
- мониторинг контрольных точек;
- анализ данных мониторинга и оценка степени соответствия информационной безопасности университета принятой Политике информационной безопасности.

3.6. Показателями качества обеспечения безопасности информационных ресурсов и процессов являются:

- формализованные оценки состояния информационной безопасности подразделений университета по результатам периодических проверок. Оценка отражает степень соответствия организации защиты информационных активов университета нормативным документам по обеспечению ИБ.

3.7. Результаты мониторинга в виде обобщенной информации, а также результаты аудита на соответствие настоящему Положению, должны регулярно докладываться ректору.

3.8. Методическое руководство и контроль выполнения требований настоящего Положения осуществляет директор департамента цифрового развития и информатизации.

3.9. Методики, периодичность (регулярность) контрольных мероприятий устанавливаются ОССА ДЦРИ.

4. ПОРЯДОК ВВОДА В ДЕЙСТВИЕ И ПЕРЕСМОТРА ПОЛОЖЕНИЯ

4.1. Настоящее Положение утверждается ректором университета и вводится в действие соответствующим распоряжением.

4.2. Поводом для пересмотра Положения могут являться, в частности:

- изменения действующей нормативно-правовой базы;
- изменения организационной структуры университета;
- изменения научных и учебно-образовательных процессов университета.

4.3. Порядок пересмотра настоящего Положения:

- начальник отдела сетевого и системного администрирования ДЦРИ собирает предложения по изменению документа от заинтересованных сторон;
- директор департамента цифрового развития и информатизации составляет проект новой редакции Положения;
- выполняется процедура согласования;
- документ направляется на утверждение ректору.

4.4. Настоящее Положение должно пересматриваться совместно с документами, содержащими требования ИБ к процедурам обеспечения ИБ не реже одного раза в три года.

4.5. Все изменения в Положение вносятся соответствующим приказом ректора.

5. ОТВЕТСТВЕННОСТЬ ЗА РЕАЛИЗАЦИЮ ПОЛОЖЕНИЯ

5.1. Вопросы Положения по мониторингу информационной безопасности и контролю защитных мер в целом курирует директор департамента цифрового развития и информатизации, а отдельные ее направления по поручению директор департамента цифрового развития и информатизации – работники ОССА ДЦРИ.

5.2. Ответственность за реализацию и актуализацию настоящего Положения несет директор департамента цифрового развития и информатизации (сотрудники, его замещающие).

5.3. Координация и контроль распределения ролей и ответственностей по вопросам мониторинга ИБ и контроля защитных мер осуществляется начальником ОССА ДЦРИ по согласованию с директором департамента цифрового развития и информатизации.

5.4. Руководители структурных подразделений университета несут ответственность за то, что:

- применяемые ими меры обеспечения информационной безопасности соответствуют данному Положению;
- требования безопасности при использовании СКЗИ выполняются;
- лица, ответственные за работу с Федеральным казначейством, осведомлены, что данные активы информационной системы университета должны быть доступны только уполномоченным работникам.

5.5. Нарушения данного Положения должны быть предметом разбирательств, по результатам которых должны быть приняты соответствующие меры.