МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

Рег. от 02.07.2020 № 12-50-71

УТВЕРЖДАЮ
Ректор
_____ Н.Ю. Анисимов
«02» июля 2020 г.

ПОЛИТИКА
информационной безопасности ДВФУ

ПТ-ДВФУ-520/2-2020

Процесс	П-7 «Управление инфраструктурой»
Держатель документа	Проректор по экономике и финансам
Ответственность за использование действующей версии документа несёт его пользователь	
Ответственность за использование действующей версии документа несёт его пользователь. Действующая версия документа находится в СЭД «DIRECTUM» / Общая папка / Реестр ВНД ДВФУ / Действующие; СЭД «DIRECTUM» / Общая папка/ Библиотека изменений	

Владивосток
2020

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности ДВФУ определяет цели и задачи информационной безопасности федерального государственного автономного образовательного учреждения высшего образования «Дальневосточный федеральный университет» (далее соответственно – Политика информационной безопасности, ДВФУ/Университет), устанавливает основные методы её обеспечения и организацию управления информационной безопасностью Университета.

1.2. Настоящая Политика информационной безопасности утверждается взамен Политики информационной безопасности ДВФУ (ПТ-ДВФУ-520-2017), утвержденной приказом от 24.10.2017 № 12-13-2084.

1.3. Руководители структурных подразделений Университета несут персональную ответственность за обеспечение выполнения требований информационной безопасности в возглавляемых ими подразделениях.

1.4. Работники Университета обязаны соблюдать требования настоящей Политики информационной безопасности и иных документов, регламентирующих деятельность в области информационной безопасности.

1.5. Настоящая Политика информационной безопасности разработана в соответствии с законодательством Российской Федерации, нормами права в части обеспечения информационной безопасности, нормативными актами Правительства Российской Федерации, нормативными актами федеральных органов исполнительной власти в области защиты информации и основывается в том числе на следующих актах:

– Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 05.12.2016 № 646;

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

– Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической

информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

– ГОСТ Р ИСО 9001-2015. Национальный стандарт Российской Федерации. Системы менеджмента качества. Требования (далее – ГОСТ Р ИСО 9001-2015);

– ГОСТ Р ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;

– ГОСТ Р ИСО/МЭК 27002-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (далее – ГОСТ Р ИСО/МЭК 27002-2012);

– ГОСТ Р ИСО/МЭК 27005-2010. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21;

– Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 25.12.2017 № 239.

1.6. Контроль за выполнением требований настоящей Политики информационной безопасности осуществляет лицо, уполномоченное ректором ДВФУ, курирующее вопросы в сфере информационной безопасности.

1.7. Политика информационной безопасности не распространяется на вопросы по защите государственной тайны в ДВФУ.

1.8. Положения настоящей Политики информационной безопасности применимы для использования во внутренних нормативных и методических документах Университета, а также в договорах (контрактах).

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящей Политике информационной безопасности используются следующие термины:

Аудит информационной безопасности Университета – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самим Университетом (внутренний аудит), так и независимыми внешними организациями (внешний аудит) в том числе на основе ГОСТ Р ИСО 9001-2015 и ГОСТ Р ИСО/МЭК 27002-2012.

Группа реагирования на инциденты информационной безопасности – группа квалифицированных и доверенных сотрудников Университета, которая выполняет, координирует и поддерживает реагирование на нарушения информационной безопасности, затрагивающие информационные системы ДВФУ.

Информационный технологический процесс – часть производственного технологического процесса, содержащая операции над информацией, необходимой для функционирования Университета.

Информационная безопасность – состояние защищенности информационных активов Университета в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т. п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов Университета. Защищенность достигается обеспечением совокупности свойств информационной безопасности – конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры Университета.

Информационные активы Университета – активы Университета, имеющие отношение к его информационной сфере и представляющие ценность с точки зрения достижения уставных целей.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению конфиденциальности, целостности, доступности информационных активов Университета.

Критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Мониторинг информационной безопасности Университета – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности Университета, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы, информационные услуги и пр.

Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления ДВФУ, отнесенные к указанной категории специально созданной комиссией.

Риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Субъекты Университета – сотрудники, обучающиеся, контрагенты Университета, а также инициируемые от их имени действия над объектами информационной системы.

Угроза – опасность, предполагающая возможность потерь (ущерба).

Управление информационной безопасностью Университета – совокупность целенаправленных действий, осуществляемых в рамках настоящей Политики информационной безопасности в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер).

3. ЦЕЛИ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УНИВЕРСИТЕТА

3.1. Целями защиты информации Университета являются:

– предотвращение или снижение ущерба от инцидентов информационной безопасности;

– достижение адекватности мер по защите от угроз информационной безопасности;

– обеспечение стабильности функционирования Университета в целом;

– выполнение требований действующего законодательства Российской Федерации по защите информации.

3.2. Задачами деятельности по обеспечению информационной безопасности Университета являются:

– мониторинг состояния информационных систем ДВФУ и систем обеспечения информационной безопасности Университета;

– своевременное выявление, оценка и прогнозирование потенциальных угроз информационной безопасности и уязвимостей объектов защиты;

– создание эффективного механизма оперативного реагирования на угрозы и инциденты информационной безопасности, в том числе силами группы реагирования на инциденты информационной безопасности;

– повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности с учетом требований системы менеджмента качества;

– выработка рекомендаций по устранению уязвимостей.

4. ОБЪЕКТЫ ЗАЩИТЫ

Объектами защиты системы информационной безопасности в Университете являются:

1) информационные активы, содержащие информацию ограниченного распространения:

– персональные данные;

– сведения, составляющие коммерческую тайну;

– служебная информация;

2) объекты критической информационной инфраструктуры;

3) открыто распространяемая информация, необходимая для функционирования Университета, независимо от формы и вида ее представления;

4) пользователи информационных систем Университета;

5) информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникаций, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

5. КОНЦЕПТУАЛЬНАЯ СХЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УНИВЕРСИТЕТА

5.1. Концептуальная схема информационной безопасности Университета направлена на защиту ее информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий пользователей и иных лиц, технических сбоев,

неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

5.2. Стратегия Университета в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности (от организационных мер на уровне руководства Университета до специализированных мер информационной безопасности по каждому выявленному в Университете риску), основанных на оценке рисков информационной безопасности.

5.3. Для противодействия угрозам информационной безопасности в Университете на основе имеющегося опыта составляются модели предполагаемых угроз и модели нарушителей. Чем точнее сделан прогноз (составлены модели угроз и нарушителей), тем эффективнее может быть создана система защиты информации при минимальных ресурсных затратах.

5.4. Действия пользователей могут иметь непреднамеренный ошибочный или иной характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией пользователей и их способностью к адекватным действиям в нештатной ситуации.

5.5. На основании данных, получаемых в ходе периодического мониторинга и аудита информационных систем Университета, в случае изменения технологических процессов, возникновения новых угроз или изменения их характера, модели угроз и нарушителя могут быть пересмотрены.

6. ОСНОВНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Мониторинг – контроль состояния защитных мер, влияющих на информационную безопасность, с возможностью блокирования нежелательных действий и быстрого восстановления рабочих параметров информационной системы.

6.2. Персонификация и адекватное разделение ролей и ответственности между работниками Университета исходя из принципа персональной и единоличной ответственности за совершаемые операции.

6.3. Организация доступа пользователей к информационным активам (системам) Университета в соответствии с политикой разграничения доступа.

6.4. Разработка и внедрение защитных мер, адекватных характеру угроз, с учетом совместимости этих мер с действующим технологическим процессом и затрат на их реализацию. При этом меры, принимаемые

для обеспечения информационной безопасности, не должны усложнять достижение уставных целей Университета, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности для субъектов Университета.

6.5. В случае возникновения инцидента информационной безопасности, по согласованию с лицом, уполномоченным ректором ДВФУ, курирующим вопросы в сфере информационной безопасности, для всестороннего установления его причин и условий, а также лиц, виновных в нарушении установленных правил, по инициативе подразделения, ответственного за обеспечение информационной безопасности в ДВФУ, может быть проведена служебная проверка. По результатам проверки нарушитель может быть привлечен к ответственности. Непосредственные руководители лиц, нарушивших требования локальных актов в сфере организации информационной безопасности в ДВФУ, также могут быть привлечены к ответственности, в случае установления факта недостаточного контроля с их стороны за исполнением пользователями требований локальных актов в сфере обеспечения информационной безопасности в ДВФУ.

6.6. С целью профилактики и урегулирования нарушений в области информационной безопасности в ДВФУ создается и действует Комиссия по урегулированию инцидентов информационной безопасности, деятельность которой регламентируется отдельным внутренним нормативным документом.

7. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ

7.1. Модели угроз и нарушителей являются определяющими при проектировании, создании, поддержании и совершенствовании системы обеспечения информационной безопасности Университета.

7.2. Источники угроз, уязвимости и объекты нападений, пригодные для реализации угрозы, типы возможных потерь, масштабы потенциального ущерба определяются моделью угроз безопасности информации.

8. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Требования по обеспечению информационной безопасности Университета разрабатываются исходя из проводимого моделирования угроз безопасности информации с соблюдением требований действующего законодательства Российской Федерации, нормативных актов федеральных органов исполнительной власти в области защиты информации.

8.2. Общие требования по обеспечению информационной безопасности формулируются внутренними нормативными документами Университета для следующих областей:

– защита персональных данных;
– организация хранения персональных данных;
– обеспечение безопасности критической информационной инфраструктуры;
– организация защиты детей от информации, распространяемой посредством информационно-телекоммуникационных сетей, причиняющей вред здоровью и (или) развитию детей;
– организация работы автоматизированных рабочих мест;
– подключение к корпоративной вычислительной сети;
– организация парольной защиты;
– организация работы в компьютерных классах;
– использование корпоративной электронной почты;
– использование программного обеспечения;
– организация антивирусной защиты;
– порядок использования ресурсов сети Интернет;
– использование средств криптографической защиты информации;
– управление информационными потоками, взаимодействие с информационными системами сторонних организаций (внешними информационными системами) и правила и процедуры применения удаленного доступа;
– проведение аудита автоматизированных рабочих мест;
– выявление, анализ, устранение уязвимостей;
– реагирование на инциденты информационной безопасности;
– контроль состава технических средств, программного обеспечения и средств защиты информации;
– резервирование технических средств, программного обеспечения, баз данных, средств защиты информации и их восстановления при возникновении нештатных ситуаций;
– организация работы сайта;
– организация видеонаблюдения в Университете;
– запись и обработка телефонных переговоров.

9. ОРГАНИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

9.1. В целях выполнения задач по обеспечению информационной безопасности, в соответствии с международными и российскими стандартами по безопасности, в Университете функционирует структурное подразделение, ответственное за обеспечение информационной безопасности. Контроль за исполнением задач данного структурного подразделения возложен на лицо, уполномоченное ректором ДВФУ, курирующее вопросы в сфере информационной безопасности.

9.2. Основной целью данного структурного подразделения является обеспечение деятельности Университета по реализации текущей Политики информационной безопасности в соответствии с уставными целями Университета.

9.3. Лицо, уполномоченное ректором ДВФУ, курирующее вопросы в сфере информационной безопасности, осуществляет обеспечение структурных подразделений ДВФУ товарами и услугами, относящимися к сфере информационных технологий. Структурные подразделения, определенные лицом, уполномоченным ректором ДВФУ, курирующим вопросы в сфере информационной безопасности, обеспечивают работоспособность информационной инфраструктуры Университета и информационных систем, их отказоустойчивость и беспрерывную работу.

10. АУДИТ И САМООЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. Порядок и периодичность проведения аудита информационной безопасности Университета, а также отдельных его структурных подразделений определяется лицом, уполномоченным ректором ДВФУ, курирующим вопросы в сфере информационной безопасности, на основании потребности в такой деятельности.

10.2. Внешний аудит информационной безопасности проводится независимыми организациями, имеющими право на осуществление такой деятельности, с целью проверки и оценки ее соответствия требованиям действующего законодательства Российской Федерации в области информационной безопасности. Внешний аудит информационной безопасности проводится на основании приказа лица, уполномоченного ректором ДВФУ, курирующего вопросы в сфере информационной безопасности.

10.3. Самооценка уровня информационной безопасности и внутренний контроль соблюдения требований информационной безопасности проводится

структурным подразделением, ответственным за обеспечение информационной безопасности, с целью выявления и регистрации недостатков защитных мер и оценки полноты реализации положений текущей Политики информационной безопасности, инструкций и руководств по обеспечению информационной безопасности Университета. Самооценка уровня информационной безопасности и внутренний контроль проводится по решению лица, уполномоченного ректором ДВФУ, курирующего вопросы в сфере информационной безопасности.

10.4. При подготовке к внешнему аудиту информационной безопасности необходимо проведение самооценки информационной безопасности.

11. УПРАВЛЕНИЕ ПОЛИТИКОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11.1. Настоящая Политика информационной безопасности, изменения и дополнения к ней утверждаются ректором или иным уполномоченным в установленном порядке лицом.

11.2. Ответственность за поддержание Политики информационной безопасности в актуальном состоянии несет держатель документа.

11.3. Контроль за размещением на официальном сайте ДВФУ в сети Интернет актуальной версии Политики информационной безопасности осуществляет держатель документа.

11.4. Подлинник настоящей Политики информационной безопасности хранится в Отделе документационного обеспечения и контроля Организационно-административного департамента согласно утвержденной номенклатуре дел.

11.5. Порядок периодической проверки документа (либо внесения в документ изменений, прекращения его действия) определен Регламентом управления внутренними нормативными документами в действующей редакции.

11.6. Настоящая Политика информационной безопасности подлежит обязательной рассылке проректорам, директорам школ/филиалов, руководителям структурных подразделений.