СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

СТАНДАРТ ОРГАНИЗАЦИИ

СТО 6.5-1

Политика информационной безопасности

Регистрационный номер документа	
Структурное подразделение	
Уполномоченный по качеству	
Дата получения	

Комсомольск-на-Амуре
2014

СТАНДАРТ ОРГАНИЗАЦИИ

Система менеджмента качества **ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**	**СТО 6.5-1** **Введен впервые**

СОГЛАСОВАНО

Первый проректор

_____ И.В. Макурин

«28» ноября 2014 г.

Начальник ИТ-Управления

_____ Е.Б. Абарникова

«28» ноября 2014 г.

Начальник организационно-правового управления

_____ Н.А. Лашкина

«28» ноября 2014 г.

УТВЕРЖДАЮ

Ректор университета

_____ Э.А. Дмитриев

«28» ноября 2014 г.

Комсомольск-на-Амуре
2014

Введен приказом № 461а-О от 28.11.2014

Содержание

1 Назначение и область применения

1.1 Назначение

Настоящий документ описывает политику информационной безопасности ФГБОУ ВО «КнАГТУ». (**Изм. № 1**)

Целью разработки данного стандарта является закрепление подходов к функционированию и совершенствованию системы обеспечения информационной безопасности в ФГБОУ ВО «КнАГТУ» (**Изм. № 1**) и определяет:

– цели и задачи системы обеспечения информационной безопасности;

– основные принципы и общие требования по обеспечению информационной безопасности;

– организацию системы обеспечения информационной безопасности.

1.2 Область применения

Требования настоящего стандарта распространяются на всех сотрудников ФГБОУ ВО «КнАГТУ» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.). (**Изм. № 1**)

2 Нормативные ссылки

Настоящий стандарт разработан в соответствии со следующими документами:

Конституция Российской Федерации.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Постановление Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012 г. № 1119.

Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. № 21.

Приказ ФСБ России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах

персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10 июля 2014 г. № 378.

3 Термины, определения, сокращения

3.1 Термины и определения

В настоящем стандарте применяются следующие термины с соответствующими определениями:

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Владелец информационного ресурса – подразделение Университета, наделенное полномочиями владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец информационного ресурса определяется на этапе создания соответствующего ресурса.

Данные – информация, представленная в электронной форме.

Доступность – обеспечение возможности легитимным пользователям за приемлемое время получать требуемую информационную услугу.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Идентификация риска – процесс выявления и классификации рисков.

Информационная безопасность – состояние и режим эксплуатации средств хранения, доставки и автоматизированной обработки, при котором обеспечивается уровень защиты информационных ресурсов, достаточный для минимизации ущерба, вызванного возможными нарушениями

безопасности.

Информационный ресурс – различная информация Университета на всех этапах ее жизненного цикла, обеспечивающая основную деятельность Университета и представляющая ценность с точки зрения достижения поставленных целей.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационный риск (ИТ-риск, риск автоматизации процессов) – риск, связанный с использованием информационных технологий, неудовлетворительным состоянием автоматизированных информационных систем Университета.

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности. Нарушение может быть вызвано ошибками персонала, неправильным функционированием технических средств, природными факторами, преднамеренными злоумышленными действиями, приводящими к нарушению доступности, целостности, конфиденциальности информации.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность – обеспечение доступности информации только ограниченному кругу лиц, имеющих соответствующие полномочия.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Критичный информационный ресурс (критичная информация) – информация, создание, модификация и обработка которой связаны с повышенным риском информационной безопасности.

Критичные операции – операции, связанные с повышенными рисками информационной безопасности.

Критичные процессы/системы – процессы/системы, связанные с использованием критичных информационных ресурсов.

Критичные уязвимости – недостатки и ошибки системного и прикладного программного обеспечения на всех уровнях архитектуры автоматизированных информационных систем, создающие повышенные риски информационной безопасности критичным информационным ресурсам.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила

разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В данном документе оператором выступает Университет.

Операционный риск – риск, возникающий в результате недостатков в организации деятельности Университета, используемых технологиях, функционировании информационных систем, неадекватных действий или ошибок сотрудников, а также в результате внешних событий.

Оценка риска – оценка вероятности реализации риска и величины возможных потерь при реализации конкретного вида риска и/или совокупных рисков, принимаемых на себя Университетом.

Риск – возможность возникновения у Университета потерь (убытков), незапланированных расходов или возможность снижения планируемых доходов.

Риск информационной безопасности – риск, являющийся составной частью ИТ-риска, возникающий вследствие наличия угроз безопасности информационным ресурсам Университета.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования

информационной системы.

Руководство – Ректорат университета.

Система обеспечения информационной безопасности – часть общей системы управления Университета, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности Университета. Включает структуру, политики, совокупность мероприятий, методов и средств, обеспечивающих требуемый уровень безопасности информационных ресурсов участниками соответствующих процессов.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Угроза информационной безопасности – внешний или внутренний фактор, создающий риск информационной безопасности.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Университет – ФГБОУ ВО «Комсомольский-на-Амуре государственный технический университет». **(Изм. № 1)**

Уязвимость – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы информационной безопасности.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

3.2 Сокращения

В настоящем стандарте применяются следующие сокращения:

АВПО – антивирусное программное обеспечение;
АРМ – автоматизированное рабочее место;
ИТ (IT) – информационные технологии;
ИСПДн – информационная система персональных данных;
ЛВС –локальная вычислительная сеть;
НСД – несанкционированный доступ;
ОС – операционная система;
ПДн – персональные данные;
ПО – программное обеспечение;
СЗИ – средства защиты информации;
СЗПДн – система (подсистема) защиты персональных данных;
СИБ – служба информационной безопасности;
СУБД – система управления базами данных;
ТКУИ – технические каналы утечки информации;
УБПДн – угрозы безопасности персональных данных;
ЭП – электронная подпись.

4 Ответственность

4.1 Все сотрудники университета несут ответственность за выполнение требований настоящей политики.

4.2 Сотрудники университета, нарушающие требования информационной безопасности и руководители подразделений, не обеспечивающие их выполнение, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

4.3 Контроль за выполнением требований настоящей политики возлагается на руководство университета, руководство ИТ-управления, руководителей всех структурных подразделений университета.

5 Цели и задачи системы обеспечения информационной безопасности

5.1 Цель системы обеспечения информационной безопасности – создание и постоянное соблюдение в Университете условий, при которых риски, связанные с нарушением безопасности информационных ресурсов Университета, постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска.

Процессы обеспечения информационной безопасности Университета являются составной и неотъемлемой частью процессов управления

информационными технологиями и сопутствующими операционными рисками и осуществляются на основе циклической модели: “планирование - реализация - проверка - совершенствование - планирование - …”.

5.2 Безопасность информационных ресурсов Университета оценивается и обеспечивается по каждому из следующих аспектов:

– доступность;
– целостность;
– конфиденциальность.

При этом критерием оценки является вероятность, размер и последствия нанесения Университету любого вида ущерба (невыполнение имеющихся перед государством и контрагентами обязательств, финансовые потери, репутационные потери и прочее).

5.3 Состояние информационной безопасности оказывает непосредственное влияние на операционные риски деятельности Университета, в связи с чем, любой факт (инцидент) нарушения информационной безопасности рассматривается как существенное событие.

5.4 Задачами системы обеспечения информационной безопасности являются:

– снижение рисков Университета, связанных с использованием информационных технологий;
– создание условий для максимальной автоматизации выполнения различных операций Университета и исключения ручных операций при условии минимизации рисков;
– своевременное выявление новых угроз;
– контроль состояния информационной безопасности на всех этапах жизненного цикла автоматизированных информационных систем;
– минимизация потерь Университета при реализации угроз информационной безопасности;
– обеспечение жизнедеятельности Университета и безопасности его информационных ресурсов в условиях форс-мажорных обстоятельств (экономические и политические кризисы, природные и техногенные катастрофы, террористические угрозы и пр.);
– оптимизация затрат на обеспечение информационной безопасности.

6 Основные принципы обеспечения информационной безопасности

Университет определяет следующие основные принципы обеспечения информационной безопасности:

Осведомленность о риске информационной безопасности. Процессы обеспечения информационной безопасности затрагивают каждого сотрудника Университета, использующего его информационные ресурсы, и накладывают на него соответствующие обязанности и ограничения.

Персональная ответственность. Ответственность за нарушения требований информационной безопасности возлагается непосредственно на сотрудников, допустивших нарушения, и руководителя подразделения, в котором нарушения допущены.

Минимальность полномочий. Любому сотруднику Университета доступ к информационным ресурсам предоставляется только в том объеме, который необходим ему для выполнения служебных обязанностей. Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными процедурами.

Комплексность защиты. Меры по обеспечению безопасности информационных ресурсов принимаются по всем идентифицированным видам угроз с учетом результатов оценки рисков информационной безопасности.

Адекватность защиты. Принимаемые меры обеспечения информационной безопасности эффективны и соразмерны имеющим место рискам информационной безопасности.

Эргономичность защиты. Средства защиты должны быть максимально “прозрачными” и удобными для пользователей и администраторов автоматизированных систем.

Документированность. Документирование обеспечивает закрепление достигнутого текущего состояния системы обеспечения информационной безопасности. Любые изменения этого состояния оформляются документально.

Непрерывность процессов контроля и совершенствования системы обеспечения информационной безопасности. В Университете осуществляется постоянный мониторинг и аудит системы обеспечения информационной безопасности, по результатам которых осуществляется анализ эффективности принятых мер обеспечения информационной безопасности с учетом изменений IT-среды, появления новых угроз, инцидентов и проблем, планируются и внедряются дополнительные меры защиты.

Контроль со стороны руководства. Руководство на регулярной основе рассматривают отчеты о состоянии информационной безопасности в подразделениях Университета и фактах нарушений установленных требований, а также общие и частные вопросы информационной безопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы. Политика

информационной безопасности и предложения по ее актуализации рассматриваются Руководством на периодической основе.

Целевое финансирование мероприятий по обеспечению информационной безопасности. Ежегодный бюджет Университета предусматривает специальные статьи расходов на обеспечение информационной безопасности.

7 Основные принципы реализации процедур оценки рисков

В связи с трудоемкостью и субъективностью оценки рисков информационной безопасности, а также с учетом необходимости унификации и максимального удешевления технологий защиты, в Университете осуществляется:

– категорирование информационных ресурсов по степени их критичности. Категорирование осуществляется СИБ совместно с подразделением - владельцем информационного ресурса по каждому из аспектов информационной безопасности: доступности, целостности и конфиденциальности;

– использование типовых требований безопасности, дифференцированных по категориям информационных ресурсов. Выполнение типовых требований обеспечивает соответствующий базовый уровень информационной безопасности для каждой категории информационных ресурсов;

– использование типовых средств и процедур обеспечения информационной безопасности для разных информационных ресурсов одной категории;

– использование моделей злоумышленника адекватных реальным угрозам;

– оценка достаточности базового уровня безопасности с учетом конкретных особенностей применяемых информационных технологий и связанных с ними угроз.

В случае недостаточности, по результатам проведенного анализа рисков, обеспечиваемого базового уровня безопасности осуществляется определение дополнительных требований и мер обеспечения информационной безопасности.

8 Источники угроз

Любое лицо, имеющее логический или физический доступ к информационным ресурсам и компонентам соответствующих информационных технологий (программному обеспечению и данным,

средствам вычислительной техники, коммуникационному оборудованию и каналам связи) может являться потенциальным злоумышленником. При этом предполагается возможность сговора сотрудника Университета с внешним злоумышленником, но не сговор двух и более сотрудников Университета.

Целью злоумышленника является получение контроля над информационным ресурсом, приводящего к нарушению его доступности, целостности или конфиденциальности.

Для достижения целей злоумышленник может использовать все экономически соизмеримые с потенциальным ущербом способы проведения атак на всех уровнях архитектуры информационных систем.

Источниками угроз информационным ресурсам Университета являются:

- внешние и внутренние злоумышленники;
- ошибочные действия персонала;
- вирусные атаки;
- отказы и сбои оборудования и программного обеспечения;
- техногенные и природные катастрофы;
- террористические угрозы.

9 Общие требования по обеспечению информационной безопасности

В основе процессов управления информационной безопасностью Университета лежат следующие общие требования:

9.1 Назначение и распределение ролей, и обеспечение доверия к персоналу

«Ролевое» управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных системах.

Роли формируются с учетом принципа минимальности полномочий.

Ни одна роль не должна позволять пользователю проводить единолично критичные операции.

Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в автоматизированных системах без непосредственного доступа к данным.

В критичных системах по решению владельца информационного ресурса может вводиться роль администратора информационной безопасности автоматизированной системы, в функции которого входит

подтверждение прав и полномочий пользователей, заведенных в системе ее администратором.

Должностные обязанности сотрудников и трудовые договоры предусматривают обязанности персонала по выполнению требований по обеспечению информационной безопасности.

Приказы и распоряжения, актуальная информация по вопросам обеспечения информационной безопасности, в том числе по выявленным нарушениям, доводятся до всех сотрудников Университета под роспись.

9.2 Управление доступом к информационным ресурсам и регистрация

Все информационные ресурсы Университета идентифицируются, категорируются и имеют своих владельцев.

Доступ к информационным ресурсам всем сотрудникам Университета предоставляется только на основании документально оформленных заявок, согласованных с их владельцами. По умолчанию определяется отсутствие доступа.

Доступ к информационным ресурсам не предоставляется (прекращается) в случае отсутствия производственной необходимости, изменения функциональных и должностных обязанностей, увольнения сотрудника.

Проводится периодический формальный контроль соответствия согласованных и реальных прав доступа к информационным ресурсам текущему статусу пользователя.

Прямой доступ пользователей к базам данных не предоставляется.

Доступ ко всем информационным ресурсам Университета осуществляется только после авторизации пользователя.

Журналы аудита действий пользователей и администраторов автоматизированных систем должны быть информативны, защищены от модификации и храниться в течение срока, потенциально необходимого для использования при расследовании возможных инцидентов, связанных с нарушением информационной безопасности.

9.3 Управление жизненным циклом автоматизированных систем

Процедуры по обеспечению информационной безопасности предусматриваются на всех стадиях жизненного цикла автоматизированных систем: при разработке (приобретении), эксплуатации, модернизации, снятии с эксплуатации.

Разработка, тестирование автоматизированных систем отделяются от эксплуатации.

Разработчики программного обеспечения не допускаются к его промышленной эксплуатации.

Разработка и тестирование программного обеспечения проводятся на

выделенных физически или логически средствах вычислительной техники (виртуальные серверы), не использующихся для промышленной эксплуатации автоматизированных систем.

В контрактах со сторонними разработчиками на поставку систем предусматривается их ответственность за наличие в системах скрытых недокументированных возможностей, ведущих к ущербу Университета, а также соблюдение условий конфиденциальности.

Все изменения, вносимые в автоматизированные системы, контролируются и документируются. Дистрибутивные комплекты и исходные тексты систем собственной разработки, а также дистрибутивные комплекты приобретаемых систем хранятся в ИТ-Управлении.

В состав документации на критичные автоматизированные системы в обязательном порядке входит документация по обеспечению ее информационной безопасности.

Ввод автоматизированных систем в эксплуатацию производится только после их аттестации на соответствие предъявленным требованиям по информационной безопасности. Не допускается эксплуатация автоматизированных систем, не прошедших аттестации или имеющих неустраненные критичные замечания.

При выводе автоматизированной системы из эксплуатации или замене входящего в ее состав оборудования осуществляется принудительное удаление информации с соответствующих машинных носителей и из памяти компьютеров за исключением ведущихся в установленном порядке контрольных архивов электронных документов.

9.4 Антивирусная защита

Каждый сотрудник Университета обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной безопасности в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать СИБ при подозрениях на вирусное заражение.

Техническая возможность подключения пользователями к рабочим станциям ЛВС внешних накопителей информации, модемов, мобильных телефонов, беспроводных интерфейсов, использование CD-/DVD-дисководов максимально ограничивается.

Антивирусная защита обеспечивается использованием в Университете специализированного программного обеспечения.

Для снижения влияния человеческого фактора, исключения возможности отключения или отсутствия обновления антивирусных средств, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производится централизованно в

автоматизированном режиме. При этом обеспечивается минимально возможный период обновления.

При невозможности централизованного обновления антивирусного и системного ПО периодичность, сроки и порядок проведения соответствующих мероприятий определяются оценкой имеющихся рисков вирусного заражения критичных информационных ресурсов и техническими возможностями такого обновления.

9.5 Безопасное использование ресурсов Интернет

Использование ресурсов Интернет в подразделениях Университета разрешается исключительно в производственных целях.

Взаимодействие с контрагентами по сети Интернет осуществляется с использованием специализированных систем и средств защиты, аттестованных на соответствие требованиям информационной безопасности.

Использование рабочих станций с доступом к ресурсам Интернет для обработки критичной информации запрещается.

Порядок публикации информации в сети Интернет определяется отдельными регламентами. Обсуждение сотрудниками Университета на форумах и в конференциях сети Интернет вопросов, касающихся их служебной деятельности, допускается только при наличии соответствующих указаний руководства.

Доступ сотрудников к ресурсам сети Интернет санкционируется руководством и согласовывается службой информационной безопасности, которая осуществляет контроль за соблюдением сотрудниками требований информационной безопасности, включая контентный анализ сообщений.

На узлах доступа в сеть Интернет принимаются необходимые меры для противодействия хакерским атакам и распространению спама.

9.6 Использование средств криптографической защиты информации

Применение средств криптографической защиты информации для обеспечения безопасности информационных ресурсов Университета и взаимодействия со сторонними организациями производится в соответствии с порядком, установленным государственными уполномоченными органами.

Использование средств ЭП обеспечивает целостность электронного документа и подтверждение авторства подписавшей его стороны и является лучшей практикой организации электронного документооборота при взаимодействии с контрагентами.

Во внутренних системах Университета механизмы криптографического контроля целостности используются в зависимости от результатов оценки рисков информационной безопасности.

Конфиденциальность информации при передаче по публичным

сетям и внешним каналам связи обеспечивается обязательным применением шифрования.

Риски, связанные с возможной компрометацией криптографических ключей или доступом к защищаемой информации в обход средств криптографической защиты, должны минимизироваться специальными техническими и организационными мерами.

Криптографические ключи, предназначенные для защиты электронного документооборота Университета со сторонними организациями, изготавливаются сторонами самостоятельно.

9.7 Обеспечение непрерывности бизнеса и восстановления после сбоев

Непрерывность критичных процессов при наступлении отказов и сбоев обеспечивается резервированием оборудования, каналов связи, резервным копированием информации, регулярной проверкой их работоспособности и адекватности. Процедуры восстановления после сбоев документируются в соответствующих регламентах и планах.

9.8 Обеспечение физической безопасности

Помещения Университета категорируются в зависимости от критичности размещаемых в них хранилищ информационных ресурсов. В соответствии с категорией обеспечивается техническая укрепленность помещений, оснащение средствами видеоконтроля, контроля доступа, пожаротушения и сигнализации.

9.9 Защита персональных данных

9.9.1 Система защиты персональных данных (СЗПДн), строится на основании:

- частной модели актуальных угроз и вероятного нарушителя;
- положения об обработке персональных данных;
- положения по защите персональных данных;
- нормативных документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Университета. На основании анализа актуальных угроз безопасности ПДн описанного в Частной модели актуальных угроз и вероятного нарушителя, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по внутреннему контролю за соблюдением безопасности персональных данных.

Организационные мероприятия должны включать:

- правовое основание для сбора персональных данных;
- определение ответственных лиц за соблюдением мер

безопасности;

– защиту персональных данных, обрабатываемых без средств автоматизации;

– защиту персональных данных, обрабатываемых с применением средств автоматизации;

– защиту объектов от хищения;

– защиту съемных накопителей, содержащих персональные данные;

– вопросы уничтожения персональных данных.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

– защиты от несанкционированного доступа к персональным данным;

– антивирусной защиты для рабочих станций пользователей и серверов;

– межсетевого экранирования;

– обнаружения вторжений;

– контроля защищенности персональных данных;

– криптографической защиты информации, при передаче защищаемой информации по каналам связи;

– защиты среды виртуализации;

– защиты от утечки по ТКУИ.

9.9.2 СЗПДн может включать в себя следующие подсистемы:

Идентификации и аутентификации субъектов доступа и объектов доступа. Подсистема обеспечивает присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Управления доступом субъектов доступа к объектам доступа. Подсистема обеспечивает управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивает контроль за соблюдением этих правил.

Ограничения программной среды. Подсистема обеспечивает установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения

Регистрации событий безопасности. Подсистема обеспечивает сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Антивирусной защиты. Подсистема обеспечивает обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Обнаружения (предотвращения) вторжений. Подсистема обеспечивает обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

Контроля (анализа) защищенности персональных данных. Подсистема обеспечивает контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Обеспечения целостности информационной системы и персональных данных. Подсистема обеспечивает обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Обеспечения доступности персональных данных. Подсистема обеспечивает авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Защиты среды виртуализации. Подсистема исключает несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым

операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Защиты технических средств. Подсистема исключает несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, обеспечивает защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Защиты информационной системы, ее средств, систем связи и передачи данных. Подсистема обеспечивает защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Выявления инцидентов и реагированию на них. Подсистема обеспечивает обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Управления конфигурацией информационной системы и системой защиты персональных данных. Подсистема обеспечивает управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

9.9.3 В ИСПДн Университета выделяют следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администраторы безопасности ИСПДн;
- пользователи ИСПДн;
- системные администраторы.

Администратором безопасности является штатный сотрудник Университета, ответственный за функционирование СЗПДн, назначается приказом Ректора.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и

протоколирования и к части ключевых элементов ИСПДн;

– не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

– реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;

– осуществлять аудит средств защиты;

– устанавливать доверительные отношения своей защищенной сети с другими защищенными сетями.

Пользователем ИСПДн является штатный сотрудник Университета, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

– располагает конфиденциальными данными, к которым имеет доступ.

Системным администратором является штатный сотрудник Университета или лица сторонних организаций, осуществляющих свои функции на основании двухстороннего договора. Системный администратор не имеет полномочий для управления подсистемами обработки данных и безопасности.

Системный администратор обладает следующим уровнем доступа и знаний:

– обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

– обладает частью информации о технических средствах и конфигурации ИСПДн;

– имеет физический доступ к техническим средствам обработки информации и средствам защиты;

– знает, по меньшей мере, одно легальное имя доступа.

10 Организация системы обеспечения информационной безопасности

10.1 Управление системой обеспечения информационной безопасности осуществляет руководство Университета:

– утверждение и пересмотр политики информационной безопасности Университета;

– организация процесса управления информационной безопасностью в Университете, включая определение подразделений, ответственных за управление отдельными процессами обеспечения информационной безопасности, утверждение положений о них;

– обеспечение условий и утверждение бюджета для эффективной реализации политики информационной безопасности;

– анализ отчетов о состоянии информационной безопасности Университета.

10.2 Все подразделения Университета и их руководители отвечают за реализацию политики информационной безопасности и управление процессами ее обеспечения в рамках своей компетенции:

10.2.1 ИТ-Управление:

– разрабатывает нормативные, инструктивные и методические документы Университета по обеспечению информационной безопасности;

– разрабатывает требования по защите информационных ресурсов в аспектах целостности и конфиденциальности на основе анализа рисков информационной безопасности;

– осуществляет контроль соответствия требованиям на всех стадиях жизненного цикла автоматизированных систем, от проектирования до снятия с эксплуатации;

– обеспечивает управление ключевыми системами средств криптографической защиты;

– организует проведение единой антивирусной политики в Университете;

– организует работу и осуществляет взаимодействие с администраторами ИТ-Управления;

– проводит расследования инцидентов и фактов нарушений информационной безопасности и информирует руководство о результатах проведенного расследования;

– организует обучение персонала по вопросам информационной безопасности;

– осуществляет инструментальный контроль и мониторинг текущего состояния информационной безопасности;

– регулярно информирует руководство о состоянии информационной безопасности в Университете, в том числе, в составе сводных отчетов;

– обеспечивает взаимодействие с уполномоченными государственными органами по вопросам информационной безопасности;

– осуществляет анализ, оценку и прогноз риска, связанного с нарушением информационной безопасности Университета.

– обеспечивает выполнение требований информационной безопасности при подключении и администрировании коммуникационного оборудования, операционных систем, СУБД и систем доставки;

– проводит обновление системного ПО, связанное с устранением критичных уязвимостей;

– обеспечивает доступность информационных ресурсов в условиях отказов и других неблагоприятных событий в части коммуникационного оборудования, операционных систем, СУБД и систем доставки.

– обеспечивает выполнение требований информационной безопасности при администрировании автоматизированных информационных систем;

– обеспечивает хранение программной документации;

– осуществляет регистрацию информации об инцидентах, имеющих отношение к информационной безопасности;

– обеспечивает доступность информационных ресурсов в условиях отказов и других неблагоприятных событий в части автоматизированных информационных систем Университета.

10.2.2 Все подразделения Университета:

– совместно с ответственными сотрудниками ИТ-Управления проводят категорирование информационных ресурсов, владельцами которых они являются, и определяют те из них, которые являются критичными;

– совместно с ответственными сотрудниками ИТ-Управления участвуют в оценке рисков реализации угроз их информационным ресурсам;

– устанавливают в пределах своей компетенции режим и порядок доступа, правила работы с информационными ресурсами, владельцами которых они являются;

– обеспечивают выполнение требований и процедур информационной безопасности при работе сотрудников с информационными ресурсами Университета.

– обеспечивают учет в подразделении информационных ресурсов и сотрудников, имеющих к ним доступ;

– обеспечивают инструктаж сотрудников по вопросам информационной безопасности;

– обеспечивают контроль проведения антивирусных мероприятий в подразделении и соблюдения требований информационной безопасности;

– обеспечивают взаимодействие с ответственными сотрудниками ИТ-Управления при инцидентах информационной безопасности.

11 Разработчики

Данный документ разработали:

Начальник ИТ-Управления	Е.Б. Абарникова
Ведущий специалист по информационной безопасности ОССА ИТ-Управления	Д.С. Магола

Лист регистрации изменений

	Номер приказа, дата утверждения изменений	Количество страниц изменения	Дата получения изменения	Подпись уполномоченного по качеству
1	№ 100-О от 15.03.2016	-	15.03.2016	Короткова М.В.

Введен приказом № 461а-О от 28.11.2014