Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение
высшего образования
«Самарский государственный экономический университет»

ПРИКАЗ

Самара

№ 257 - ОВ **«26» апреля 2023года**

По общим вопросам

Об утверждении политики информационной безопасности ФГАОУ ВО «СГЭУ»

В целях выполнения требований Федерального Закона от 14.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказа Федерального Агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», приказа Федеральной службы безопасности от 09.02.2005 №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический университет».
2. Помощнику проректора по административной работе О.Ю.Семыкиной разместить документ в Единой правовой базе в разделе «Информационная безопасность».
3. Считать утратившим силу приказ от 29 декабря 2016 года №644-ОВ «Политика информационной безопасности ФГБОУ ВО «Самарский государственный экономический университет».
4. Контроль за исполнением настоящего приказа оставляю за проректором по безопасности и управлению хозяйственным комплексом А.А. Максимовым.

Врио ректора Е.А. Кандрашина

Разработал: Начальник ОИБ С.П. Ткаченко

(846) 933-88-09 (вн.502)

Федеральное государственное
автономное образовательное
учреждение высшего образования
«Самарский государственный
экономический университет»

УТВЕРЖДЕНО
приказом врио ректора
ФГАОУ ВО «СГЭУ»

№ 257-01 от 26.04. 2023 г.

Политика
информационной безопасности Федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический Университет»

1. Введение

Политика информационной безопасности (далее – Политика) Федерального государственного автономного образовательного учреждения высшего образования «Самарский государственный экономический университет» (далее - Университет) определяет систему взглядов на проблему обеспечения информационной безопасности (далее – ИБ). Политика представляет собой систематизированное изложение целей и задач защиты, которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы обеспечения информационной безопасностью (далее – СОИБ) Университета.

Обеспечение ИБ – необходимое условие для успешного осуществления уставной деятельности Университета и включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Университет.

Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических, организационных мероприятий и финансовых затарат.

2. Обозначения и сокращения

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
КЭП	Квалифицированная электронная подпись

НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СОИБ	Система обеспечения информационной безопасности

3. Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищённость информации от нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного тиражирования.

Бизнес-процесс – последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Университета.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения ими в пределах, установленных законом.

Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

Доступность информации – состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации – деятельность Университета по принятию правовых, организационных и технических мер направленных на защиту информации от неправомерного доступа.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения информационных ресурсов Университета.

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

Информационный процесс – процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационный ресурс (актив) – массив информации, который находится в распоряжении Университета и представляет ценность.

Инцидент – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).
Инцидент информационной безопасности – одно или серия нежелательных, или неожиданных событий ИБ, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу ИБ.
Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.
Конфиденциальная информация – информация с ограниченным доступом или ПДн, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.
Конфиденциальность информации – состояние защищённости информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.
Мобильный код – несамостоятельное программное обеспечение или компонент программного обеспечения (скрипты, макросы, иные компоненты) получаемые из мест распространения мобильного кода, передаваемые по сети и выполняемые на компонентах ИС (в местах использования мобильного кода) без предварительной установки (инсталляции) пользователем для расширения возможностей системного и (или) прикладного программного обеспечения.
Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.
Управление риском – процесс выбора и реализации мер по модификации (снижению) риска.
Политика ИБ – общие цели и указания, формально выраженные руководством Университета в отношении защиты ИС от НСД .
Привилегии – это права доверенного объекта(субъекта) на совершение каких-либо действий по отношению к объектам системы.
Риск – сочетание вероятности события и его последствий.
Система обеспечения информационной безопасности (СОИБ) – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.
Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, в полном объёме реализующий полномочия владения, пользования, распоряжения указанными объектами.
События информационной безопасности – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.
Угроза – опасность, предполагающая возможность потерь (ущерба).

Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

4. Цель

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, репутационного или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ.

Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- соответствие требованиям Федерального законодательства, нормативно методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
- обеспечение непрерывности критических бизнес-процессов;
- достижение адекватности мер по защите от угроз ИБ;
- изучение партнёров, клиентов, конкурентов и кандидатов на работу;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;

5. Основания для разработки

Настоящая политика разработана на основе требований законодательства Российской Федерации, накопленного в Университете опыта в области обеспечения ИБ, интересов и целей Университета. При написании отдельных положений настоящей политики использовались следующие нормативные документы:

- Федеральный Закон от 14.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Приказ Федерального Агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ Федеральной службы безопасности от 09.02.2005 №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»;
- ГОСТ Р ИСО/МЭК 27001-2021 «Методы и средства обеспечения безопасности»;
- РС БР ИББС-2.5-2014 «Менеджмент инцидентов информационной безопасности».

6. Область действия

Настоящая Политика распространяется на все бизнес-процессы Университета и обязательна для применения всеми сотрудниками и руководством Университета, а также пользователями его информационных ресурсов. Настоящая политика распространяется на информационные системы Университета.

Лица, осуществляющие разработку внутренних документов Университета, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

7. Содержание политики

7.1. Система обеспечения информационной безопасностью

Для достижения указанных целей и задач в Университете внедряется СОИБ. СОИБ документирована в настоящей политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех работников Университета в области действия системы. Документированные требования СОИБ доводятся до сведения работников Университета. Средства обеспечения ИБ внедряются по результатам проведения оценки рисков нарушения информационной безопасности. Стоимость внедряемых средств обеспечения ИБ не должна превышать возможный ущерб, возникающий при реализации угроз.

7.1.1. Структура документов

В целях создания взаимосвязанной структуры нормативных документов Университета в СОИБ, разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:

- Политика ИБ.
- Инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников Университета по реализации Политики ИБ.
- Отчётные документы о выполнении требований ИБ.

7.1.2. Ответственность за обеспечение ИБ

Для эффективного функционирования СОИБ функции обеспечения ИБ в части криптографической защиты информации и работе с ПДн возложены на проректора по безопасности и управлению хозяйственным комплексом в подчинении которого находится отдел информационной безопасности, а в части правомерности управления доступом к информационным ресурсам Университета на проректора по научной работе и инновационному развитию в подчинении которого находится отдел технического администрирования.

На отдел ИБ и отдел технического администрирования Управления информационных систем и технологий возлагается решение следующих основных задач:

- проведение в жизнь Политики ИБ;
- определение требований к СКЗИ;
- контроль и оценка эффективности применяемых СКЗИ;
- расследования инцидентов информационной безопасности;
- организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;
- оказание методической помощи сотрудникам в вопросах обеспечения ИБ;
- регулярная оценка и управление рисками ИБ в соответствии с установленными процедурами в области управления рисками;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения ИБ;
- обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов;
- информирование, обучение и повышение квалификации работников Университета в сфере ИБ;

- сбор, накопление, систематизация и обработка информации по вопросам ИБ;
- обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений.

Для решения возложенных задач, сотрудники отделов технического администрирования и отдела ИБ, имеют следующие права:

- определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей ИС в указанной области;
- получать информацию от пользователей ИС Университета по любым аспектам применения ими информационных технологий в Университете;
- участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании, разработке и внедрении новых ИС;
- участвовать в испытаниях ИС по вопросам оценки качества реализации требований по обеспечению безопасности информации;
- контролировать деятельность пользователей по вопросам обеспечения ИБ;
- готовить предложения руководству по обеспечению требований ИБ.

7.2. Объект защиты

7.2.1. Ответственность за ресурсы

В Университете должны быть оценены с точки зрения их важности все ресурсы. Для всех ценных ресурсов должен быть составлен реестр (перечень). Благодаря информации о ресурсах Университета реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

В ИС Университета присутствуют следующие типы информационных ресурсов содержащие:

- конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Университета;
- криптографическую информацию, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, объекты и помещения, в которых размещены такие системы.
- информацию о ПДн, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;
- информацию открыто распространяемую, необходимую для работы Университета, независимо от формы и вида её представления;

7.2.2. Классификация информации

Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена руководством Университета. Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация должна пересматриваться для поддержания актуальности её соответствия с категорией ресурса. Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку (гриф).

7.3 Оценка и обработка рисков

В Университете должны быть определены требования к безопасности путём методической оценки рисков. Оценки рисков должны определить количество и расположить по приоритетам выявленные риски в соответствии с критериями принятия рисков и бизнес-целями Университета. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков. Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков.

Оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

- учесть изменения бизнес-требований и приоритетов;
- принять во внимание новые угрозы и уязвимости;
- убедиться в том, что реализованные средства защиты информации сохранили свою эффективность.

Перед обработкой каждого риска Университет должен выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для Университета. Такие решения должны регистрироваться.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

- применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска, если он точно удовлетворяет Политике Университета и критериям принятия рисков;
- уклонение от риска путём недопущения действий, которые могут быть его причиной;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

7.4 Безопасность персонала

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с Политикой ИБ Университета, должны быть доведены до сотрудника при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как общие обязанности по реализации и поддержке политики безопасности, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

7.4.1. Условия найма

Все принимаемые на работу сотрудники должны выразить согласие и подписать свои трудовые договоры, в которых устанавливается их ответственность за ИБ. В договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Университета по проверке выполнения требований ИБ, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения сотрудником требований ИБ. Обязанности по обеспечению ИБ должны быть включены в должностные инструкции каждого сотрудника Университета. Все принимаемые сотрудники должны быть ознакомлены под роспись с перечнем информации, ограниченного доступа, с установленным режимом доступа с ней и с мерами ответственности за нарушение этого режима. При предоставлении сотруднику доступа к ИС Университета он должен ознакомиться под роспись с инструкцией пользователя ИС.

7.4.2. Ответственность руководства

Руководство Университета должно требовать от всех сотрудников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в Университете политиками и процедурами. Уполномоченные руководством Университета сотрудники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- выполнения действующих инструкций по вопросам ИБ;
- данных, находящихся на носителях информации;
- порядка использования сотрудниками информационных ресурсов;
- содержания служебной переписки.

7.4.3. Обучение ИБ

Все сотрудники должны проходить периодическую подготовку в области политики и процедур ИБ, принятых в Университете. План обучения составляет отдел ИБ.

7.4.4. Завершение или изменение трудовых отношений

При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

7.5 Физическая безопасность

7.5.1. Защищённые области

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Университета, места обработки ПДн должны быть размещены в защищённых областях, которые образуют контролируемые зоны. Такими средствами являются: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации. Контролируемые зоны должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающим возможность доступа только авторизованного персонала. Запрещается приём посетителей в помещениях внутри контролируемой зоны. Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, металлическими шкафами или шкафами, оборудованными замком. Помещения должны быть обеспечены средствами уничтожения документов.

7.5.2. Области общего доступа

Места доступа, через которые неавторизованные лица могут попасть в помещения Университета, должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа.

7.5.3. Вспомогательные службы.

Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС Университета.

7.5.4. Утилизация или повторное использование оборудования.

Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все конфиденциальные данные и лицензионное ПО. Отсутствие такой информации на носителях должно быть проверено отделом технического администрирования Управления информационных систем и технологий Университета, о чём должна быть сделана отметка в акте списания.

Удаление криптографической информации и ПО осуществляется сотрудниками отдела информационной безопасности согласно «Инструкции о порядке учета выдачи и уничтожения средств криптографической защиты информации».

7.5.5. Перемещение имущества

Оборудование, информация или ПО должны перемещаться за пределы Университета только при наличии письменного разрешения руководства. Сотрудники, имеющие право перемещать оборудование и носители информации за пределы Университета, должны быть чётко определены. Время перемещения оборудования за пределы Университета и время его возврата должны регистрироваться.

7.6 Контроль доступа

Основными пользователями информации в информационной системе Университета являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями. Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламенту предоставления доступа пользователей. Каждому пользователю, допущенному к работе с конкретным информационным активом Университета, должно быть сопоставлено персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать с ИС. В случае производственной необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имён (учётных записей). Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

В общем случае запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или учебы (труда) (например, компьютерные классы (посменное дежурство), использование общей учётной записи должно сопровождаться отметкой в журнале учёта машинного времени, которая должна однозначно идентифицировать текущего владельца учётной записи в каждый момент времени. Одновременное использование одной общей пользовательской учётной записи разными пользователями запрещено. Регистрируемые учётные записи подразделяются на:

- пользовательские – предназначенные для аутентификации пользователей в ИС Университета;
- системные – используемые для нужд операционной системы;
- служебные – предназначенные для функционирования отдельных процессов или приложений.

  Системные учётные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему. Служебные учётные записи используются только для запуска и работы сервисов или приложений. Использование системных или служебных учётных записей для регистрации пользователей в системе категорически запрещено.

Процедуры регистрации и блокирования учётных записей пользователей должны применяться с соблюдением следующих правил:

- использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершёнными ей действиями;
- использование групповых ID разрешать только в случае, если это необходимо для выполнения задачи;
- предоставление и блокирование прав должны быть санкционированы и документированы;
- предоставление прав доступа к ИС, только после согласования с администратором данной ИС;
- регистрация и блокирование учётных записей допускается с отдельного разрешения руководства Университета;
- уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;
- согласование изменения прав доступа с отделом технического администрирования Управления информационных систем и технологий и отделом ИБ если такое разграничение затрагивает Политику обработки ПДн и/или криптографические средства обработки информации;
- документальная фиксация назначенных пользователю прав доступа;
- ознакомление пользователей под подпись с письменными документами, в которых регламентируются их права доступа;
- предоставление доступа с момента завершения процедуры регистрации;
- обеспечение создания и поддержания формального списка всех пользователей, зарегистрированных для работы с ИС или сервисом;
- немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из Университета;
- аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;
- обеспечение того, чтобы лишние ID пользователей не были доступны другим пользователям;
- обеспечить возможность предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путем суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

7.6.1. Управление привилегиями

Доступ сотрудника к информационным ресурсам Университета должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный сотрудник, и администраторами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами. Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий.
Должны быть реализованы следующие этапы:

- идентифицированы привилегии доступа, связанные с каждым системным продуктом, например, с операционной системой, системой управления базой данных и каждым приложением, а также пользователи, которым они должны быть предоставлены;

данных и каждым приложением, а также пользователи, которым они должны быть предоставлены;

- идентифицированы привилегии пользователя на основании «производственной необходимости» необходимой для достижения поставленных целей, например, привилегии, минимально необходимые для выполнения их функциональных обязанностей, только тогда, когда эти привилегии необходимы;
- регламентирован процесс регистрации всех предоставленных привилегий и создание отчетов по ним, привилегии нельзя предоставлять до завершения процесса их регистрации; уникальные привилегии должны присваиваться на другой ID пользователя, не тот, который используется при обычной работе пользователя.

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Университета осуществляется в процессе аудита ИБ в соответствии с Правилами аудита ИБ и установленными процедурами.

7.6.2. Управление паролями

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

- все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;
- при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;
- временные пароли должны назначаться пользователю только после его идентификации;
- необходимо избегать передачи паролей с использованием третьих лиц или не зашифрованной электронной почтой;
- временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;
- пользователь должен подтвердить получение пароля;
- пароли должны храниться в электронном виде только в защищенной форме;
- назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;
- необходимо установить требования к длине пароля, набору символов и числу попыток ввода;
- необходимо изменять пароль пользователя не реже одного раза в 90 дней.

При необходимости можно рассмотреть возможность использования других технологий идентификации и аутентификации пользователей, в частности, биометрических технологий, проверки подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

7.6.3. Контроль прав доступа

Чтобы обеспечить эффективный контроль доступа необходимо ввести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

- права доступа пользователей должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИС;

- права доступа пользователей должны проверяться и переназначаться при изменении их должностных обязанностей в Университете, а также при переходе с одной работы на другую в пределах Университета;
- проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться чаще (не реже одного раза в 3 месяца);
- регулярно проверяться адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;
- должно протоколироваться изменение привилегированных учетных записей.

При выполнении процедур управления доступом пользователей должен осуществляться контроль:

- над добавлением, удалением и изменением идентификаторов, аутентификацию данных и иных объектов идентификации;
- проверки подлинности пользователей перед сменой паролей;
- блокирования прав доступа при увольнении;
- блокирования учётных записей, неактивных более 45 дней;
- включения учётных записей, используемых поставщиками для удалённой поддержки, только на время выполнения работ;
- отслеживания удалённых учётных записей, используемых поставщиками, во время работ;
- предотвращения повторного использования идентификатора пользователя и (или) устройства в течение не менее трёх лет;
- ознакомления с правилами и процедурами аутентификации всех пользователей, имеющих доступ к сведениям ограниченного распространения;
- использования механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;
- разрешения запросов и прямого доступа к базам данных только для администраторов баз данных;
- блокирования учётной записи на период равный 30 минутам или до разблокировки учётной записи администратором;
- блокирования учетных записей пользователей при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации.

7.6.4. Использование паролей

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых сотруднику Университета предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) сотрудником информации. Не допускается использование различными пользователями одних и тех же учётных данных. Первоначальное значение пароля учетной записи пользователя устанавливает отдел технического администрирования Управления информационных систем и технологий.

После первого входа в систему и в дальнейшем пароли выбираются пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля должны присутствовать три из четырёх видов символов:
- буквы в верхнем регистре;
- буквы в нижнем регистре;

- цифры;
- специальные символы (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /);

Пароль не должен содержать легко вычисляемые сочетания символов:

- имена, фамилии, номера телефонов, даты;
- последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.);
- общепринятые сокращения («USER», «TEST» и т.п.);
- повседневно используемое слово, например, имена или фамилии друзей, коллег, актёров или сказочных персонажей, клички животных;
- компьютерный термин, команда, наименование компаний, web сайтов, аппаратного или программного обеспечения;
- что-либо из вышеперечисленного в обратном написании;
- что-либо из вышеперечисленного с добавлением цифр в начале или конце;
- при смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях;
- для различных ИС необходимо устанавливать собственные, отличающиеся пароли.

Сотруднику запрещается:

- сообщать свой пароль кому-либо;
- указывать пароль в сообщениях электронной почты;
- хранить пароли, записанные на бумаге, в легко доступном месте;
- использовать тот же самый пароль, что и для других систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.);
- использовать один и тот же пароль для доступа к различным корпоративным ИС.
- производить несанкционированное распространение справочной информации, которая становится доступна при подключении к корпоративной ИС Университета.

Сотрудник обязан:

- в случае подозрения на то, что пароль стал кому-либо известен, немедленно сообщить сотруднику отдела технического администрирования Управления информационных систем и технологий и поменять пароль. Сообщить о факте компрометации сотруднику отдела ИБ;
- немедленно сообщить сотруднику отдела ИБ в случае получения от кого-либо просьбы сообщить пароль;
- менять пароль каждые 90 дней;
- менять пароль по требованию сотрудника отдела ИБ. После 6 неудачных попыток ввода пароля учётная запись блокируется на 10 минут. При систематической блокировке учётной записи работника (более 3 раз) обрабатывающего ПДн и/или эксплуатирующего СКЗИ оповещается отдел ИБ;
- убирать в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места документы и носители с конфиденциальной информацией;
- оставлять в состоянии выполненного выхода из системы компьютеры и терминалы, когда они находятся без присмотра;
- использовать уничтожители бумаги для утилизации конфиденциальных документов.

Сотрудники отдела ИБ Университета имеют право:

- осуществлять периодическую проверку стойкости паролей пользователей, используемых сотрудниками для доступа к ИС;

- принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей Политики.

7.7. Политика допустимого использования информационных ресурсов

Общие обязанности пользователя:

- при работе руководствоваться нормативной документацией к программному обеспечению (руководством пользователя);
- обращаться в службу поддержки пользователей или к специалистам, назначенными ответственными за системное администрирование и информационную безопасность, по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), а также за необходимой методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;
- знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;
- минимизировать вывод на печать обрабатываемую информацию.

7.7.1. Использование ПО

На АРМах Университета допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения. Запрещено незаконное хранение на жестких дисках АРМ Университета информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.). Решение о приобретении и установке программного обеспечения, необходимого для реализации учебных, финансовых, административно-хозяйственных задач принимает проректор по научной работе и инновационному развитию по представлении начальников заинтересованных подразделений.

Решение о приобретении средств криптографической защиты информации принимает проректор по защите информации и управлению хозяйственным комплексом по представлению начальника отдела ИБ.

Документы, подтверждающие покупку программного обеспечения, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся соответственно в Управлении информационных систем и технологий и отделе ИБ. Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию АРМ. Указанные работы, а также работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только сотрудниками Управления информационных систем и технологий. Сведения о вновь приобретённом программном обеспечении должны быть внесены в перечень разрешённого программного обеспечения.

7.7.2. Использование АРМ и ИС

К работе в ИС Университета допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности. Каждому сотруднику Университета, которому необходим доступ к ИС в рамках его должностных обязанностей, выдаются под роспись необходимые средства автоматизации. Ответственность по установке и поддержке всех компьютерных систем, функционирующих в Университете, возложена на отдел технического администрирования Управления информационных систем и технологий. Каждый сотрудник Университета, обеспеченный АРМ, получает персональное сетевое имя,

пароль, адрес электронной почты и личный каталог в сети, который предназначен для хранения рабочих файлов. Работа в ИС сотрудникам разрешена только на закреплённых за ними АРМ, в определённое время и только с разрешенным программным обеспечением и сетевыми ресурсами. Все АРМ, установленные в Университете, имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией, определённый в стандарте рабочих мест Университета. Изменение установленной конфигурации возможно после внесения соответствующих поправок в стандарт рабочих мест или по служебной записке, согласованной с отделом технического администрирования Управления информационных систем и технологий. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется отделом технического администрирования Управления информационных систем и технологий. Самостоятельная установка программного обеспечения на АРМ запрещена.

Установка и удаление любого программного обеспечения производится только сотрудниками отдела технического администрирования Управления информационных систем и технологий.

Комплектация персональных компьютеров аппаратными и программными средствами криптозащиты их установка и удаление, а также расположение таких компьютеров в помещениях контролируется отделом ИБ.

В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в отдел технического администрирования Управления информационных систем и технологий. Сотрудники отдела технического администрирования Управления информационных систем и технологий имеют право осуществлять контроль над установленным на компьютере программным обеспечением, и принимать меры по ограничению возможностей несанкционированной установки программ. Передача документов внутри Университета производится только посредством общих папок, а также средствами электронной почты.

При работе в ИС Университета сотрудник обязан:

- знать и выполнять требования локальных организационно-распорядительных документов Университета;
- использовать ИС и АРМ Университета исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИБ и отдел технического администрирования Управления информационных систем и технологий и отдел ИБ о любых фактах нарушения требований ИБ;
- ставить в известность отдел технического администрирования Управления информационных систем и технологий о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;
- незамедлительно выполнять предписания отдела информационной безопасности;
- предоставлять АРМ сотрудникам отдела ИБ для контроля;
- при необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;
- проинформировать отдел технического администрирования Управления информационных систем и технологий в случае необходимости продолжения работы по окончании рабочего дня.

При использовании ИС Университета запрещено:

- использовать АРМ и ИС в личных целях;

- отключать средства управления и средства защиты, установленные на рабочей станции;
- передавать конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с отделом ИБ и отделом технического администрирования Управления информационных систем и технологий;
- использовать информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;
- распространять угрожающую, клеветническую, непристойную информацию;
- самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС Университета;
- предоставлять сотрудникам Университета (за исключением администраторов ИС и ИБ) и третьим лицам доступ к своему АРМ;
- запускать на АРМ ПО, не входящее в Реестр разрешенного к использованию ПО;
- защищать информацию, способами, не согласованными с отделом технического администрирования Управления информационных систем и технологий;
- самостоятельно подключать рабочую станцию и прочие технические средства к корпоративной ИС Университета;
- осуществлять поиск средств и путей повреждения, уничтожения технических средств и ресурсов ИС или осуществлять попытки несанкционированного доступа к ним;
- использовать для выполнения служебных обязанностей локальные (не доменные) учетные записи АРМ.

Информация о посещаемых ресурсах ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Университета. Все электронные сообщения и документы в электронном виде, передаваемые посредством ИС Университета, подлежат обязательной проверке на отсутствие вредоносного ПО.

7.7.3. Использование ресурсов локальной сети

Для выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Университета, базы данных, электронная почта. Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы. Доступ сотрудников к ресурсам сети осуществляется согласно матрице доступа. Временное расширение прав доступа осуществляется отделом технического администрирования Управления информационных систем и технологий Университета в соответствии с Порядком предоставления (изменения) полномочий пользователя.

7.7.4. Обработка конфиденциальной информации

При обработке конфиденциальной информации сотрудники обязаны:

- знать и выполнять требования Инструкции по работе с конфиденциальной информацией;
- применять средства защиты от неавторизованного доступа при необходимости размещения конфиденциальной информации на открытом ресурсе корпоративной сети Университета;
- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;

• не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;

• проверять адреса получателей электронной почты на предмет правильности их выбора; не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;

• не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС; не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD – диски, Flash – устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

7.7.5. Использование электронной почты

Электронная почта используется для обмена в рамках ИС Университета и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде. Для обеспечения функционирования электронной почты допускается применение ПО, входящего в реестр разрешённого к использованию ПО.

При работе с корпоративной электронной почтой Университета пользователь должен учитывать:

• электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;

• электронная почта не является средством передачи информации, гарантирующим конфиденциальность передаваемой информации (передачу конфиденциальной информации вне локальной сети Университета необходимо осуществлять только в зашифрованном виде);

• электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

Организацией и обеспечением порядка работы электронной почты в Университете занимается отдел технического администрирования Управления информационных систем и технологий. Каждый сотрудник Университета получает почтовый адрес вида name@sseu.ru в домене Университета. Адрес электронной почты выдаётся сотрудником отдела технического администрирования Управления информационных систем и технологий при начальной регистрации пользователя в домене Университета. Корпоративная электронная почта Университета предназначена исключительно для использования в служебных целях. Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Университету. Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты принадлежат Университету и являются неотъемлемой частью его производственного процесса. Любые сообщения корпоративной электронной почты могут быть перлюстрированы, использованы в интересах Университета либо удалены уполномоченными сотрудниками Университета. Пользователям корпоративной электронной почты Университета запрещено вести частную переписку с использованием средств корпоративной электронной почты Университета. К частной переписке относится переписка, не связанная с исполнением сотрудником своих должностных обязанностей. Использование корпоративной электронной почты Университета для частной переписки сотрудником, надлежащим образом, ознакомленным с данной Политикой, является нарушением трудовой дисциплины Университета. Подписываясь в ознакомлении с настоящей Политикой, сотрудник даёт согласие на ознакомление и иное использование в интересах Университета его переписки, осуществляемой с использованием корпоративной

электронной почты, и соглашается с тем, что любое использование его переписки, осуществляемой с использованием корпоративной электронной почты, не может рассматриваться как нарушение тайны связи. Каждый сотрудник Университета имеет право на просмотр либо иное использование в интересах Университета сообщений корпоративной электронной почты, которые направлены или получены им, соответственно, с его или на его корпоративный электронный адрес. Использование сообщений корпоративной электронной почты осуществляется уполномоченными сотрудниками Университета в соответствии с их функциями, определёнными в данной Политике и в иных локальных нормативных актах Университета. Просмотр и иное использование сообщений электронной почты в интересах Университета осуществляется сотрудниками Университета в целях обеспечения защиты конфиденциальных сведений, обеспечения нормальной работоспособности системы электронной почты, в рамках обслуживания сервисов электронной почты, при выполнении ручной пересылки сообщений, приходящих на корпоративные электронные адреса Университета сотрудникам или группам сотрудников, а также по мотивированным запросам прямых или непосредственных руководителей любых сотрудников, чью почту необходимо использовать в интересах Университета. Использование сообщений корпоративной электронной почты в интересах Университета, в том числе ознакомление с содержанием сообщений, осуществляется в соответствии с правами доступа к информации, установленными внутренними Положениями о конфиденциальной информации и иными правовыми актами, регламентирующими порядок обращения с информацией ограниченного доступа.

Исходящие электронные сообщения сотрудников Университета должны содержать следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (вложенные файлы);
- подпись отправителя;
- предупреждение о служебном характере сообщения и его конфиденциальности.

Формат подписи отправителя:

С уважением, <Фамилия имя> <Должность> <Структурное подразделение> <Наименование Университета> <Адрес> <номера контактов: телефон, мессенджеры, адреса электронной почты> <сайт>

Формат предупреждения о служебном характере сообщения и его конфиденциальности: «Это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию. Настоящим уведомляем Вас о том, что, если это сообщение не предназначено Вам, использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых действий на основе этой информации, строго запрещено и защищается законодательством Российской Федерации. Если Вы получили это сообщение по ошибке, пожалуйста, сообщите об этом отправителю по электронной почте и удалите это сообщение. CONFIDENTIALITY NOTICE: This email and any files attached to it are confidential. If you are not the intended recipient you are notified that using, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited and protected by the laws of the Russian Federation. If you have received this email in error please notify the sender and delete this email.»

При формировании ответов на полученные электронные сообщения можно использовать следующую упрощённую подпись:

С уважением, <Фамилия имя> <Номера телефонов, мессенджеры, адреса электронной почты>

В случае получения служебного сообщения о невозможности доставки сообщения адресату или получения извещения от адресата о том, что он не получил отправленное ему сообщение, необходимо связаться с сотрудником отдела технического администрирования Управления информационных систем и технологий. Отказ от дальнейшего предоставления сотруднику Университета услуг электронной почты может быть вызван нарушениями требований настоящей политики. Прекращение предоставления сотруднику Университета услуг электронной почты наступает при прекращении действия трудового договора (контракта) сотрудника.

7.7.6. Работа в сети

Доступ к сети Интернет предоставляется сотрудникам Университета в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам. Для доступа сотрудников Университета к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.

При использовании сети Интернет необходимо:

- соблюдать требования настоящей Политики;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел технического администрирования Управления информационных систем и технологий о любых фактах нарушения требований настоящей Политики;

При использовании сети Интернет запрещено:

- использовать предоставленный Университетам доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Университета;

Публиковать, загружать и распространять материалы, содержащие:

- конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с отделом технического администрирования Управления информационных систем и технологий;
- угрожающую, клеветническую, непристойную информацию;
- вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;
- фальсифицировать свой IP- адрес, а также прочую служебную информацию.

Университет оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Блокирование и ограничение доступа пользователей к Интернет-ресурсам осуществляется на основе Регламента применения категорий Интернет-ресурсов. Информация о посещаемых сотрудниками Университета Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть

представлена Руководителям структурных подразделений, а также Руководству Университета для контроля. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

7.7.7. Использование мобильных устройств

Под использованием мобильных устройств и носителей информации в ИС Университета понимается их подключение к инфраструктуре ИС с целью обработки, приёма/передачи информации между ИС и мобильными устройствами, а также носителями информации. На предоставленных Университетам мобильных устройствах допускается использование ПО, входящего в Реестр разрешённого к использованию ПО. К предоставленным Университетам мобильным устройствам и носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ. Целесообразность дополнительных мер обеспечения ИБ определяется отделом ИБ совместно с отделом технического администрирования Управления информационных систем и технологий.

При использовании предоставленных Университетам мобильных устройств и носителей информации, сотрудник обязан:

- соблюдать требования настоящей Политики;
- использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел технического администрирования Управления информационных систем и технологий о любых фактах нарушения требований настоящей Политики;
- эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;
- обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;
- извещать отдел технического администрирования Управления информационных систем и технологий о фактах утраты (кражи) мобильных устройств и носителей информации.

При использовании предоставленных сотрудника Университета мобильных устройств и носителей информации запрещено:

- использовать мобильные устройства и носители информации в личных целях;
- передавать мобильные устройства и носители информации другим лицам (за исключением администраторов ИС и ИБ);
- оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, приём\передача информации) инициированное сотрудником Университета между ИС и неучтёнными (личными) мобильным и устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговорённых с администраторами ИС заранее). Университета оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации; Информация об использовании сотрудниками Университета мобильных устройств и носителей информации в ИС протоколируется и, при необходимости, может быть представлена руководителям структурных подразделений, а также руководству Университета. Информация, хранящаяся на предоставляемых Университетам мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО. В случае увольнения, предоставленные ему мобильные устройства и носители информации изымаются.

7.7.8. Защита от вредоносного ПО

Отдел технического администрирования Управления информационных систем и технологий регулярно проверяет сетевые ресурсы Университета антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник Университета должен незамедлительно оповестить об этом отдел технического администрирования Управления информационных систем и технологий, а в случае если на АРМ проводится обработка ПДн, то и отдел ИБ. После чего администратор АРМ должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО. В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу и немедленно поставить в известность своего руководителя и отдел технического администрирования Управления информационных систем и технологий, а также владельца файла и смежные подразделения, использующие эти файлы в работе о факте обнаружения заражения файлов вирусом.
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

Для предупреждения вирусного заражения рекомендуется:

- никогда не открывать файлы и не выполнять макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя. Удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;
- • удалять спам, рекламу и другие бесполезные сообщения;
- никогда не загружать файлы и программное обеспечение из подозрительных или неизвестных источников; периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте.
- Руководствоваться Правилами безопасности при работе с электронной почтой.

7.8 Приобретение, разработка и обслуживание систем

7.8.1. Требования безопасности для информационных систем

При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности. Требования к безопасности и средства защиты должны соответствовать ценности используемых ИС и потенциальному ущербу для Университета в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками. Системные требования к ИБ и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования ИС.

7.8.2. Корректная обработка информации

Данные, вводимые в прикладные системы, необходимо проверять, чтобы гарантировать их правильность и соответствие поставленной задаче.

7.8.3. Криптографические средства

Все, поступающие в Университет, СКЗИ должны быть учтены в соответствующем журнале поэкземплярного учёта СКЗИ. В Университете должно осуществляться управление ключами для эффективного применения криптографических

методов. Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации. Все ключи должны быть защищены от изменения, утери и уничтожения. Кроме того, секретные и закрытые ключи должны быть защищены от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено. Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса. Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты. Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям, таким как Интернет. Шифрование любой другой информации в ИС Университета должно осуществляться только после получения письменного разрешения на это.

7.8.4. Требований по обеспечению ИБ при использовании СКЗИ

СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Порядок применения СКЗИ определяется руководством Университета и должен включать:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой информацией;
- порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

При использовании шифрования в ИС Университета должны применяться только утверждённые стандартные алгоритмы и сертифицированные ФСБ и ФСТЭК России продукты, их реализующие.

7.8.5. Квалифицированные электронные подписи

(Работа с простой электронной подписью регламентируется отдельным документом)

КЭП обеспечивают защиту аутентификации и целостности электронных документов. КЭП могут применяться для любой формы документа, обрабатываемого электронным способом. Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа. При использовании КЭП, необходимо руководствоваться «Регламентом владельца квалифицированной электронной подписи ФГАОУ ВО «СГЭУ". Изготовление сертификатов для Университета производится только в Управлении Федерального казначейства по Самарской области.

7.9. Безопасность процесса внедрения ИС

Чтобы свести к минимуму вероятность повреждения ИС Университета при обновлении программного обеспечения, следует предварительно провести его тестирование в изолированной программной среде (под Windows это Sandboxie).
Для тестовой среды создается «песочница», которая должна включать:

- система и приложения;
- тестовые данные;
- сервер базы данных;
- фронтальная рабочая среда;
- клиентская операционная система;
- браузер;
- аппаратное обеспечение включает операционную систему сервера;
- сеть

7.9.1. Управление инцидентами информационной безопасности

В Университете должна быть разработана и утверждена формальная процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии. Все сотрудники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях. В дополнение к уведомлению о происшествиях ИБ и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов ИБ. Цели управления инцидентами ИБ должны быть согласованы с руководством для учёта приоритетов Университета при обращении с инцидентами. Необходимо создать механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

7.10. Управление восстановлением при нештатных ситуациях

Необходимо разработать контролируемый процесс для обеспечения и поддержки непрерывности бизнес-процессов Университета. В Университете должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить функционирование ИС и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес процессов. В плане поддержки непрерывности бизнеса должны быть чётко указаны условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях. Для каждого плана должен быть назначен определённый владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

7.11. Аудит информационной безопасности

Аудит информационной безопасности Университета должен проводить внутренние проверки СОИБ через запланированные интервалы времени.
Основные цели проведения таких проверок:

- оценка текущего уровня защищённости ИС;
- выявление и локализация уязвимостей в системе защиты ИС;

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИС;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию СОИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

В число задач, решаемых при проведении проверок и аудитов СОИБ, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно - распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления. Руководство и сотрудники Университета при проведении у них аудита СОИБ обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

7.12 Предоставление услуг сторонним организациям

7.12.1. Соглашения о предоставлении услуг

В соглашения о предоставлении услуг сторонним организациям должны быть включены требования безопасности, описание, объёмы и характеристики качества предоставляемых услуг.

7.12.2. Анализ предоставления услуг

Услуги, отчёты и записи, предоставляемые сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

- контроль объёма и качества услуг, оговоренных в соглашениях;
- предоставление сторонней организацией ФГАОУ ВО "СГЭУ" информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
- анализ предоставленных сторонними организациями отчётов о предоставленных услугах;
- управление любыми обнаруженными проблемами.

7.12.3. Приёмка систем

В Университете должен быть разработан и утверждён порядок приёмки новых ИС, обновления и новых версий ПО.

8. Ответственность

Ректор Университета определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ Университета. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СОИБ Университета лежит на руководстве отдела

технического администрирования Управления информационных систем и технологий и отдела ИБ. Все руководители несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях. Работники Университета несут персональную ответственность за соблюдение требований документов СОИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в отдел технического администрирования Управления информационных систем и технологий и отдел ИБ. В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей. Руководство Университета регулярно проводит совещания, посвящённые проблемам обеспечения информационной безопасности с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ. Нарушение требований нормативных актов Университета по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

9. Контроль и пересмотр

Общий контроль состояния ИБ Университета осуществляется Ректором. Текущий контроль соблюдения настоящей Политики осуществляет Проректор по безопасности и управлению хозяйственным комплексом. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Университета, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий. Отдел ИБ ежегодно пересматривает положения настоящей Политики. Изменения и дополнения вносятся по инициативе отдела ИБ или Проректором по безопасности и управлению хозяйственным комплексом и утверждаются Ректором.

Разработал
начальник отдела ИБ С.П.Ткаченко
вн.502