МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

ПРИКАЗ

От «16» 11 2020 г. № 436

[Об утверждении Положений]

В соответствии с решением Ученого совета университета от 25 ноября 2020 г. (протокол № 12), принятого с учетом мнения совета обучающихся,

п р и к а з ы в а ю:

1. Утвердить Положение о защите обучающихся в ФГБОУ ВО «СамГУПС» от информации, причиняющей вред их здоровью и развитию (приложение 1).
2. Положение о защите обучающихся в ФГБОУ ВО «СамГУПС» от информации, причиняющей вред их здоровью и развитию, утвержденное приказом СамГУПС № 190 от 16.03.2020 г., считать утратившим силу.
3. Утвердить Положение о политике информационной безопасности (приложение 2).
4. Приказ разместить в единой правовой базе ФГБОУ ВО «СамГУПС» (ЭИОС).
5. Контроль за исполнением настоящего приказа возложить на проректора по учебно-воспитательной работе Булатова А.А.

Ректор **И.К. Андрончев**

КОПИЯ ВЕРНА

Приложение 2
к приказу СамГУПС
от «10» 12 2020 г. № 736

ПОЛОЖЕНИЕ
о политике информационной безопасности

Термины, определения, обозначения и сокращения

В настоящей Политике использованы следующие определения:

Корпоративная информационная система - организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), программного обеспечения, баз данных, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей СамГУПС.

Персональная учетная запись (Учетная запись) - это хранимая в компьютерной системе совокупность данных о работнике или обучающемся СамГУПС, необходимая для его аутентификации и предоставления доступа к его личным данным и настройкам.

Политика информационной безопасности - система взглядов на информационную безопасность, совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации.

Пользователь - работник или обучающийся СамГУПС, получивший Учетную запись.

Простая электронная подпись - электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Частная политика информационной безопасности - система взглядов на ряд вопросов и областей информационной безопасности, которые можно объединить по какому-либо признаку.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, которая используется для определения лица, подписывающего информацию.

В настоящей Политике используются следующие сокращения:

АРМ - автоматизированное рабочее место - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

АС - автоматизированная система, состоящая из персонала и комплекса

средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

ИБ - информационная безопасность;

ИС - информационная система;

НСД - несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

Обучающийся - студент, аспирант, слушатель, экстерн;

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

САВЗ средство антивирусной защиты информации;

СЗИ средства защиты информации — технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации;

Система ИБ система информационной безопасности, обеспечивающая комплекс организационных и технических мероприятий по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

УЦТ управление цифровых технологий;

ФСТЭК Федеральная служба по техническому и экспортному контролю.

Нормативные ссылки

- Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденное Постановлением Совета Министров — Правительства Российской Федерации от 15.09.1993 № 912-51;
- Указ Президента Российской Федерации от 20.01.1994 № 170 государственной политики в сфере информатизации»;

- Указ Президента Российской Федерации от 03.04.1995 № 334 соблюдению законности в области разработки производства, реализации и шифровальных средств, а также предоставления услуг в области информации»;
- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;
- Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Требования о защите информации, не составляющей государственную тайну, содержащейся в информационных системах, утвержденные Приказом ФСТЭК России от 11.02.2013 № 17.

1 Общие положения

1.1 Настоящая Политика информационной безопасности (далее - Политика) является локальным нормативным актом СамГУПС и устанавливает общие положения по обеспечению информационной безопасности Университета.

1.2 Требования, изложенные в Политике, являются обязательными для выполнения всеми работниками Университета, при этом срочность и важность выполняемых работ не должны являться основанием для нарушения положений настоящей Политики и других документов, регламентирующих в Университете вопросы обеспечения ИБ.

1.3 Общее руководство обеспечением ИБ осуществляет ректор Университета.

1.4 Ответственность за организацию обработки персональных данных несет уполномоченное лицо Университета, назначенное приказом ректора.

1.5 Ответственность за обеспечение и контроль за соблюдением требований ИБ несет работник, назначенный приказом по Университету.

1.6 Руководители структурных подразделений Университета организуют и обеспечивают выполнение требований ИБ в своих структурных подразделениях.

1.7 Работники обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информации, соблюдать требования настоящей Политики и других документов по ИБ.

1.8 Актуализация Политики производится в обязательном порядке в следующих случаях:

а) при изменении политики Российской Федерации в области информационной безопасности, указов и законов Российской Федерации в области защиты информации;

б) при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ Университета;

в) при внесении изменений в Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в области обеспечения информационной безопасности, утвержденное распоряжением Правительства Российской Федерации от 28.05.2012 №. 856-р.

г) при выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб для Университета.

1.9 Контроль за исполнением требований Политики и поддержание ее в актуальном состоянии возлагается на начальника УЦТ.

2 Цель Политики

2.1 Основными целями Политики являются защита информации и обеспечение эффективной работы всего информационно-вычислительного комплекса Университета при осуществлении деятельности, указанной в уставе Университета.

2.2 Политика направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий работников, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

3 Задачи Политики

3.1 Описание организации системы управления ИБ Университета;

3.2 Определение частных политик ИБ, а именно:

а) политики реализации антивирусной защиты;

6) политики учетных записей;

в) политики предоставления доступа к информационному ресурсу; г) парольной политики;

д} политики защиты АРМ;

е) политики конфиденциального делопроизводства;

3.3 Определение порядка сопровождения ИС Университета.

4 Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ в Университете являются:

а) постоянный и всесторонний анализ информационного пространства Университета с целью выявления уязвимостей информационных активов;

6) своевременное обнаружение проблем, потенциально способных повлиять на ИБ Университета, и нарушителя(ей), корректировка моделей угроз;

в) разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию (при этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей Университета, а также повышать трудоемкость технологических процессов обработки информации);

г) контроль эффективности принимаемых защитных мер;

д) персонификация и адекватное разделение ролей и ответственности между работниками Университета исходя из принципа персональной и единоличной ответственности за совершаемые операции.

5 Правила обращения с конфиденциальной информацией

5.1 Обучение работников Университета правилам обращения конфиденциальной информацией проводится путем:

а) проведения специалистом по ИБ занятий с работниками, принимаемыми на работу в Университет, при наличии соответствующего запроса от руководителя подразделения на имя начальника УЦТ;

6) самостоятельного изучения работниками внутренних нормативных документов Университета.

5.2 Допуск персонала к работе с конфиденциальной информацией Университета осуществляется после ознакомления с настоящей Политикой.

Правила допуска к работе с информационными ресурсами лиц, не являющихся работниками Университета, определяются на основе договоров, заключенных с этими лицами или с организациями, представителями которых являются эти лица.

6 Защищаемые информационные ресурсы Университета

6.1 Различаются следующие категории информационных ресурсов, подлежащих защите в Университете:

6.1.1 Конфиденциальная информация - информация, определенная в соответствии с Федеральным законом от 27.07.2006 №149-ФЗ «О6 информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», указом президента Российской Федерации от 06.03.1997 № 188 ((О6 утверждении перечня сведений конфиденциального характера».

6.1.2 Открытая информация - информация, полученная от физических или юридических лиц, запрет на распространение и обработку которой был ими официально снят; информация, сформированная в результате деятельности Университета, которую запрещено относить к конфиденциальной на основании законодательства Российской Федерации; информация, представляемая в публичный доступ, используемая в хозяйственной деятельности Университета.

6.1.3 Информация ограниченного доступа - информация, не попадающая под остальные категории, доступ к которой должен быть ограничен определенным категориям лиц.

6.2 В качестве основной угрозы безопасности конфиденциальной информации, включая персональные данные, рассматривается нарушение конфиденциальности путем раскрытия ее содержимого третьим лицам, не допущенным в установленном порядке к работе с этой информацией.

6.3 Защита информации в Университете осуществляется путем исключения неправомерных или неосторожных действий со сведениями, а также с информационными ресурсами, являющимися критичными для обеспечения функционирования процессов Университета.

Для этого в Университете выполняются следующие мероприятия:

а) определяется порядок работы с документами, образцами, изделиями и другими источниками данных;

б) устанавливается круг лиц и порядок доступа к информации;

в) вырабатываются меры по контролю обращения с документами, содержащими конфиденциальные данные;

г) с работниками заключаются соглашения о неразглашении конфиденциальных сведений в соответствии с приложением Б.

6.4 Защита конфиденциальной информации, принадлежащей третьей стороне, осуществляется на основании договоров, заключаемых Университетом с данными лицами и организациями.

7 Организация системы управления информационной безопасностью Университета

7.1 Система управления информационной безопасностью Университета предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ Университета.

Для успешного функционирования Системы ИБ Университета должны быть реализованы следующие процессы:

а) определение и уточнение области действия Системы ИБ и выбор подхода к оценке рисков ИБ (определение и уточнение области действия Системы ИБ должно осуществляться на основе результатов оценки рисков, связанных с основной деятельностью Университета, а также оценки правовых рисков деятельности Университета);

б) анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов;

в) выбор и уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ;

г) принятие руководством Университета остаточных рисков и решения о реализации и эксплуатации/совершенствовании Системы ИБ (остаточные риски ИБ должны быть соотнесены с рисками деятельности Университета, и оценено их влияние на достижение целей деятельности Университета);

д) реализация системы управления ИБ.

7.2 В зависимости от специфики процесса его реализация осуществляется с соблюдением следующих этапов:

а) на этапе планирования определяется политика и методология управления рисками, а также выполняется оценка рисков, включающая в себя инвентаризацию активов, составление профилей угроз и уязвимостей, оценку эффективности контрмер и потенциального ущерба, определение допустимого уровня остаточных рисков;

б) на этапе реализации производится обработка рисков и внедрение механизмов контроля, предназначенных для их минимизации; Университетом принимается одно из четырех решений по каждому идентифицированному риску: проигнорировать, избежать, передать внешней стороне, минимизировать; после этого разрабатывается и внедряется план обработки рисков.

в) на этапе проверки отслеживается функционирование механизмов контроля, контролируются изменения факторов риска (активов, угроз, уязвимостей), проводятся аудиты и выполняются различные контролирующие процедуры.

г) на этапе действия по результатам непрерывного мониторинга и проводимых проверок выполняются необходимые корректирующие мероприятия, которые могут включать в себя, в частности, переоценку величины рисков, корректировку политики и методологии управления рисками, а также плана обработки рисков.

8 Оценка информационных рисков

8.1 Оценка информационных рисков Университета выполняется по следующим основным принципам:

а) идентификация и количественная оценка информационных ресурсов, значимых для работы Университета;

б) оценивание возможных угроз;

в) оценка существующих уязвимостей;

г) оценка эффективности средств обеспечения информационной безопасности.

При этом информационные риски зависят от:

а) показателей ценности информационных ресурсов;

б) вероятности реализации угроз для ресурсов;

в) эффективности существующих или планируемых средств обеспечения информационной безопасности.

8.2 Цель оценки рисков состоит в определении характеристик рисков информационной системы и ее ресурсов.

8.3 В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности Университета.

9 Частная политика предоставления доступа к информационным ресурсам

9.1. Частная политика предоставления доступа к информационному ресурсу определяет основные правила предоставления работникам доступа к защищаемым информационным ресурсам Университета.

9.2. Права на информационные ресурсы, разработанные работниками в соответствии с трудовыми функциями, подрядчиками и иными контрагентами, если данное условие закреплено в договоре, принадлежат Университету.

Любое размещение таких информационных ресурсов в сетях общего пользования, в том числе Интернет, без письменного согласования с ректором Университета или уполномоченным им лицом ЗАПРЕЩЕНО.

9.3. Каждому работнику Университета, допущенному к работе с конкретным информационным ресурсом, должно быть предоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым работникам могут быть представлены несколько уникальных имен (учетных записей). Использование несколькими работниками при работе в Университете одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

За создание, выдачу, изменение и приостановку действия Учетной записи отвечает УЦТ.

9.4. Предоставление (или изменение) прав доступа пользователя к учетным системам и ресурсам, не предоставляемых в рамках единого логина и пароля Университета, осуществляется на основании заявки руководителя подразделения на имя начальника УЦТ.

В заявке указывается:

а) должность, фамилия, имя и отчество работника;

6) имя пользователя (учетной записи) данного работника;

в) наименование информационного актива (системы, ресурса), к которому необходим допуск (или изменение полномочий пользователя);

г) полномочия, которых необходимо лишить пользователя или которые необходимо предоставить пользователю (путем указания решаемых пользователем задач на конкретных информационных ресурсах ИС) с указанием разрешенных видов доступа к ресурсу (ролей).

9.5. Для вновь принимаемых на работу работников и зачисленных обучающихся учетная запись создается автоматически на следующий день после утверждения приказа о принятии на работу № приказа о зачислении в Университет и активируется пользователем самостоятельно через личный кабинет, за исключением ИС, обрабатывающих конфиденциальную информацию (учетные системы).

9.6. При прекращении срока действия полномочий пользователя (окончание договорных отношений, увольнение работника) учетная запись блокируется на следующий день с момента окончания договорных отношений автоматически во всех информационных системах УЦТ.

9.7. В случае выявления передачи пароля третьим лицам или при обнаружении действий пользователя, которые могут привести к причинению прямого или косвенного ущерба Университету, уполномоченный работник УЦТ приостанавливает действие учетной записи пользователя.

9.8. Перечень сервисов Университета, в которых в соответствии со ст. 9 Федерального закона от 06.04.2011 № 63-ФЗ «О6 электронной подписи» для

обеспечения идентификации и аутентификации пользователей применяется простая электронная подпись:

9.8.1 1С: Зарплаты и кадры бюджетного учреждения (учетная ИС);

9.8.2 1С: Бухгалтерия бюджетного учреждения (учетная ИС);

9.8.3 1С: Университет ПРОФ (учетная ИС);

9.8.4 1С: Управление проектами (учетная ИС).

9.8.5 Электронная информационно-образовательная среда (MOODLE);

9.8.6 Управления научно-техническими проектами (ИС УНТП) (учетная ИС).

9.8.7 1С:Документооборот; Личный кабинет;

9.8.9 Корпоративная почта;

9.8.10 Облачные сервисы:

а) хранилища пользовательских и других файлов;

б) средства обработки информации на основе веб-интерфейса.

10 Частная политика учетных записей

10.1 Политика учетных записей определяет основные правила присвоения учетных записей пользователям информационных систем Университета.

Виды учетных записей подразделяются на:

а) пользовательские, предназначенные для идентификации и аутентификации пользователей информационных активов Университета;

б) системные, используемые для нужд операционной системы;

в) служебные, предназначенные для обеспечения функционирования отдельных процессов или приложений.

10.2 После активации учетной записи пользователю доступен функционал ИС в рамках должностных обязанностей работника Университета и академических прав и обязанностей, обучающихся Университета, а также облачные сервисы, действующие через единую учетную запись личного кабинета.

11 Частная парольная политика

11.1 Настоящая Политика определяет основные правила обращения с паролями, используемыми для доступа к защищаемым информационным системам Университета.

11.2 В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 №217, и Мерами защиты информации в государственных информационных системах, утвержденными ФСТЭК России 11.02.2014, для ИС Университета установлены требования, соответствующие классу защищенности К3.

11.3 Временный пароль должен иметь минимальную длину — 6 (шесть) символов. Временный пароль должен быть сменен пользователем при его первом обращении к ИС Университета.

11.4 Пароли учетных записей пользователей должны соответствовать следующим требованиям безопасности:

а) длина пароля должна быть не менее 8 (восьми) символов;

б) пароль должен содержать цифровые символы и буквенные символы латиницы в верхнем и нижнем регистрах;

в) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 (четырех) позициях;

г) пароль не должен совпадать с именем пользователя, а также включать в себя легко вычисляемые сочетания символов, общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), не должен содержать месяцы, годы, дни недели и т.п., фамилии, инициалы и регистрационные номера автомобилей, названия и идентификаторы организаций, номера телефонов или группы символов, состоящие из одних цифр (12345678, 11111 и т.п.).

11.5 После 5 (пяти) неудачных попыток ввода пароля в систему учетная запись соответствующего пользователя блокируется.

Снятие блокировки происходит автоматически не менее чем через 30 (тридцать) минут, или блокировка может быть снята принудительно администратором соответствующей ИС.

11.6 Требования к процессам работы со средствами криптографической защиты информации на съемных (отчуждаемых) носителях устанавливаются в соответствии с утвержденными инструкциями.

12 Частная политика реализации антивирусной защиты

12.1 Настоящая Политика определяет основные правила для реализации антивирусной защиты в Университете.

12.2 Основным способом защиты информации от воздействия компьютерных вирусов на АРМ является применение средств антивирусной защиты (далее — САВЗ).

12.3 В качестве САВЗ на АРМ используется централизованно приобретенный УЦТ программный продукт.

12.4 За непосредственное выполнение мероприятий по защите информации от воздействия компьютерных вирусов на АРМ отвечает уполномоченное лицо УЦТ.

12.5 Обновление баз вирусных сигнатур для САВЗ осуществляется по мере поступления обновлений, но не реже 1 (одного) раза в месяц.

12.6 С целью исключения проникновения вредоносных программ на АРМ все внешние машинные носители информации, такие как гибкие магнитные диски, флэш-накопители, оптические диски и т.д., при подключении к техническим средствам АРМ должны быть подвергнуты входному антивирусному контролю.

13 Частная политика защиты АРМ

13.1 Настоящая Политика определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации Университета от неавторизированного доступа, утраты или модификации.

13.2 Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

13.3 Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

13.4 Пользователи получают доступ к ресурсам вычислительной сети после ознакомления с настоящей Политикой, иными документами по обеспечению ИБ и перечнями конфиденциальной информации.

13.5 Конечным пользователям предоставляется доступ только к тому функционалу, который необходим для выполнения их должностных обязанностей.

13.6 Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

13.7 Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к уполномоченным работникам УЦТ.

13.8 Локальное техническое обслуживание должно осуществляться только при личном присутствии пользователя.

13.9 Дистанционное техническое обслуживание должно осуществляться только со специально выделенных АРМ, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться. При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и должны использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

13.10 Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя.

В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

13.11 Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

14 Частная политика сопровождения ИС

14.1 ИБ должна обеспечиваться на всех стадиях жизненного цикла ИС:

а) разработка;

б) пилотная эксплуатация;

в) промышленная эксплуатация;

г) архивная копия.

14.2 Разработка технических заданий, проектирование, создание, тестирование, приемка средств и систем защиты ИС проводятся при участии уполномоченных работников УЦТ. Порядок разработки и внедрения ИС должен быть регламентирован и контролироваться.

14.3 При разработке ИС необходимо придерживаться требований и методических указаний, определенных стандартами, входящими в группу ГОСТ 34.ххх «Стандарты информационной технологии».

14.4 Ввод в действие, эксплуатация, снятие с эксплуатации ИС в части вопросов ИБ должны осуществляться при участии уполномоченных работников УЦТ.

14.5 На стадиях, связанных с разработкой ИС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

а) неверной формулировки требований к ИС;

б) выбора некорректной модели жизненного цикла ИС, в том числе

в) некорректного выбора процессов и вовлеченных в них участников;

г) принятия неверных проектных решений;

д) внесения разработчиком дефектов на уровне архитектурных решений;

е) неполной, противоречивой и некорректной реализации требований к ИС;

ж) разработки некачественной документации;

з) установки ИС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в ИС либо к неадекватной реализации требований;

и) неверного конфигурирования ИС;

к) приемки ИС, не отвечающей требованиям заказчика.

Привлекаемые для разработки средств и систем защиты ИС на договорной основе физические и юридические лица должны иметь все необходимые разрешения на данный вид деятельности в соответствии с законодательством Российской Федерации.

14.6 При приобретении готовых ИС и их компонентов разработчиком должна быть предоставлена документация, в том числе содержащая описание защитных мер, предпринятых разработчиком в отношении угроз ИБ.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком ИС и их компонентов относительно безопасности разработки, безопасности поставки, эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости.

В договор (контракт) о приобретении ИС и их компонентов рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы.

В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающее возможность сопровождения ИС и их компонентов без участия разработчика.

Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство Университета, должно обеспечить анализ влияния угрозы невозможности сопровождения ИС и их компонентов на обеспечение непрерывности
работы.

14.7 На стадии эксплуатации должна быть обеспечена защита от следующих угроз:

а) умышленное несанкционированное раскрытие, модификация или уничтожение информации;

б) неумышленная модификация или уничтожение информации;

в) недоставка или ошибочная доставка информации;

г) отказ в обслуживании или ухудшение обслуживания.

14.8 На стадии сопровождения должна быть обеспечена защита от угроз:

а) внесения изменений в ИС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;

б) невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния ИС.

14.9 На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб Университету, и информации, используемой средствами обеспечения ИБ, из постоянной памяти ИС или с внешних носителей.

14.10 Требования ИБ должны включаться во все договоры (контракты) на проведение работ или оказание услуг, связанных с обслуживанием ИС, на всех стадиях жизненного цикла ИС.

15 Профилактика нарушений Политики

15.1 Под профилактикой нарушений Политики понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в Университете и проведение разъяснительной работы по ИБ среди пользователей.

Проведение в ИС Университета регламентных работ по защите информации предполагает выполнение процедур контрольного тестирования (проверки) функций СЗИ, что гарантирует ее работоспособность с точностью до периода тестирования.

Контрольное тестирование функций СЗИ может быть частичным или полным и должно проводиться с установленной в ИС Университета степенью периодичности.

15.2 Задача предупреждения в ИС Университета возможных нарушений информационной безопасности решается по мере наступления следующих событий:

а) включение в состав ИС Университета новых программных и технических средств (новых рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест в СЗИ ИС Университета;

б) изменение конфигурации программных и технических средств ИС (изменение конфигурации программного обеспечения рабочих станций, серверного или коммуникационного оборудования и др.) при условии появления уязвимых мест

в СЗИ ИС Университета, при появлении сведений о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения технических средств, используемых в ИС Университета.

Администратор ИБ (возможно, при помощи сторонней организации, специализирующейся в области информационной безопасности) собирает и анализирует информацию о выявленных уязвимых местах в составе операционных систем и/или программного обеспечения относительно ИС Университета.

Источниками подобного рода сведений могут служить официальные издания и публикации различных компаний, объединений и других организаций, специализирующихся в области защиты информации.

15.3 Для решения задач контроля защищенности ИС используются инструментальные средства для тестирования реализованных в составе СЗИ ИС Университета средств и функций защиты.

По результатам профилактических работ, проводимых в ИС, необходимо сделать соответствующие записи в специальном журнале Администратором ИБ.

Плановая и внеплановая разъяснительная работа по правилам настоящей политики, а также инструктаж работников/обучающихся Университета по соблюдению требований нормативных и регламентных документов по информационной безопасности, принятых в Университете, проводится при пересмотре настоящей Политики и/или при возникновении инцидента нарушения правил Политики.

16 Ликвидация последствий нарушения Политики

16.1 Администратор ИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации ИС, должен своевременно обнаруживать нарушения информационной безопасности, факты осуществления НСД к защищаемым информационным ресурсам и предпринимать меры по их локализации и устранению.

16.2 В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым информационным ресурсам ИС рекомендуется уведомить администратора ИБ и начальника УЦТ и далее следовать их указаниям.

После устранения инцидента УЦТ составляет акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также регистрирует факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

17 Ответственность за нарушение Политики

17.1 Ответственность за выполнение правил Политик безопасности в рамках своих служебных обязанностей несет каждый пользователь ИС.

17.2 Ответственность за разработку мер и контроль обеспечения защиты информации несет администратор ИБ.

17.3 Ответственность за реализацию Политики возлагается:

а) в части, касающейся разработки и актуализации правил внешнего доступа и управления доступом, антивирусной защиты - на ответственного за функционирование и безопасность средств защиты информации (администратора ИБ);

б) в части, касающейся доведения правил Политик до работников Университета - на работника отдела кадров;

в) работник несет персональную ответственность за конфиденциальность информации, доступной ему в связи с осуществлением его должностных обязанностей.

Приложение А
(обязательное)

Перечень сведений конфиденциального характера в САМГУПС

1 Сведения об обучающемся и/или поступающем, позволяющие идентифицировать его личность (персональные данные):

1.1 фамилия, имя, отчество;

1.2 пол;

1.3 дата рождения;

1.4 место рождения;

1.5 гражданство, подданство;

1.6 серия и номер основного документа, удостоверяющего личность; сведения о дате выдачи указанного документа и выдавшем его органе;

1.7 состав семьи;

1.8 адрес регистрации по месту жительства, домашний и мобильный телефон, а также адрес личной электронной почты;

1.9 результаты Единого государственного экзамена / вступительных испытаний, проводимых СамГУПС самостоятельно;

1.10 материалы вступительных испытаний;

1.11 номер учебной группы;

1.12 основа обучения (источник финансирования);

1.13 форма обучения;

1.14 факультет/институт, направление подготовки/специальность, направленность (профиль/специализация);

1.15 текущая и итоговая успеваемость;

1.16 сведения о воинском учете (для военнообязанных и лиц, подлежащих призыву на военную службу);

1.17 сведения о законных представителях;

1.18 сведения в медицинской справке о прохождении медицинского осмотра (медицинской книжке), если это требуется в связи с прохождением обучения;

1.19 сведения о документе о предыдущем уровне образования;

1.20 номер страхового индивидуального лицевого счета;

1.21 сведения о дисциплинарных взысканиях;

1.22 сведения о социальных льготах, которые предоставляются в соответствии с законодательством Российской Федерации, а также коллективными договорами и локальными нормативными актами Университета;

1.23 иные сведения, являющиеся персональными данными.

2 Сведения о работнике образовательной организации, позволяющие идентифицировать его личность (персональные данные):

2.1 фамилия, имя, отчество;

2.2 пол;

2.3 дата рождения;

2.4 место рождения;

2.5 гражданство, подданство;

2.6 серия и номер основного документа, удостоверяющего личность; сведения о дате выдачи указанного документа и выдавшем его органе;

2.7 идентификационный номер налогоплательщика;

2.8 номер страхового свидетельства государственного пенсионного страхования;

2.9 сведения о номере, дате выдачи страхового медицинского полиса и страховой компании, выдавшей его;

2.10 образование, специальность, квалификация, сведения о документе об образовании;

2.11 ученая степень, ученое звание;

2.12 стаж работы;

2.13 предыдущее место работы;

2.14 семейное положение;

2.15 состав семьи;

2.16 адрес регистрации по месту жительства, домашний телефон и мобильный телефон, а также адрес личной электронной почты;

2.17 сведения о воинском учете (для военнообязанных и лиц, подлежащих призыву на военную службу);

2.18 сведения о заработной плате;

2.19 сведения, содержащиеся в документах, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям (об инвалидности, о беременности и т.д.);

2.20 сведения о дисциплинарных взысканиях;

2.21 сведения о социальных льготах, которые предоставляются в соответствии с законодательством Российской Федерации, а также коллективными договорами и локальными нормативными актами Университета;

2.22 любые иные сведения, с которыми работник считает нужным ознакомить работодателя или в предоставлении которых работодателю возникла необходимость.

3 Тестовые задания и контрольные измерительные материалы для оценки уровня учебных достижений обучающихся, содержащиеся в банке тестовых заданий, за исключением переведенных в установленном порядке в открытый доступ, текущего календарного года на бумажных и электронных носителях.

4 Сведения о сущности изобретения, полезной модели или промышленного образца до момента официального опубликования информации о них образовательной организацией.

5 Сведения, содержащие информацию о прохождении и решениях, принимаемых на промежуточных этапах рассмотрения аттестационных дел работников.

6 Сведения, содержащие данные по результатам внутреннего и внешнего контроля объемов и качества образовательных услуг и служебным проверкам.

7 Сведения о финансовых операциях до момента их официального опубликования.

8 Сведения о состоянии банковских счетов до момента их официального опубликования.

9 Сведения о планах закупок и инвестициях до момента их официального опубликования.

10 Сведения относительно оборудования помещений охранной и пожарной сигнализацией и места ее установления.

11 Сведения об объемах поступающих средств (из бюджета, из внебюджетных фондов, от предпринимательской деятельности, от спонсоров и жертвователей) до момента их официального опубликования

12 Сведения о деятельности комиссий по осуществлению конкурентных закупок.

13 Сведения, раскрывающие содержание плана гражданской обороны образовательной организации.

14 Сведения, раскрывающие вопросы защиты образовательной организации от чрезвычайных ситуаций техногенного характера w террористической деятельности.

15 Другие сведения, связанные с деятельностью образовательной организации, которые не составляют государственную тайну, и разглашение которых может привести к причинению вреда образовательной организации, повлечь материальный, нематериальный и репетиционный ущерб.

Приложение Б
(обязательное)

Соглашение о неразглашении сведений конфиденциального характера (в том числе персональных данных) СамГУПС

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный университет путей сообщения», в лице, действующего на основании в дальнейшем именуемый «Университет» «Работодатель», с одной стороны, и в дальнейшем именуемый «Работник», с другой стороны, заключили настоящее соглашение о неразглашении информации, содержащей сведения конфиденциального характера (далее - Соглашение) о нижеследующем:

1 Работник при исполнении трудовых обязанностей имеет доступ к информации, содержащей сведения конфиденциального характера, в соответствии с Перечнем сведений конфиденциального характера Университета, и обязуется в течение всего срока действия трудовых отношений с Университетом:

а) соблюдать требования информационной безопасности, установленные Университетом в Политике информационной безопасности и иных локальных нормативных актах;

б) не разглашать информацию, содержащую сведения конфиденциального характера Университета, а также коммерческую тайну иных предприятии и организаций, переданную Работнику при исполнении трудовых обязанностей;

в) не сообщать устно или письменно кому бы то ни было информацию, содержащую сведения конфиденциального характера Университета, не раскрывать и не комментировать публично такую информацию без соответствующего разрешения имеющих на это право лиц;

г) в случае попытки посторонних лиц получить информацию, содержащую сведения конфиденциального характера Университета, немедленно сообщать об этом своему непосредственному руководителю;

д) при прекращении трудовых отношений с Университетом все материальные носители информации (бумажные документы, неутвержденные проекты бумажных документов, черновики и их копии, съемные материальные носители информации, распечатки на принтерах и пр.), которые находились в пользовании Работника в связи с выполнением должностных обязанностей, передать представителям Университета (непосредственному руководителю) в установленный ими срок;

е) об утрате или недостаче материальных носителей информации, содержащих информацию, содержащую сведения конфиденциального характера Университета, удостоверений, пропусков, ключей от сейфов (хранилищ), персональных идентификаторов, личных печатей и других фактах, которые могут привести к разглашению информации, содержащей сведения конфиденциального характера Университета, а также о причинах и условиях возможной утечки этой

информации немедленно сообщать непосредственному руководителю и лицу, ответственному за обеспечение обработки персональных данных;

ж) использовать переданные Университетом и установленные на рабочем месте технические средства обработки и передачи информации исключительно для выполнения обязанностей, предусмотренных заключенным с Университетом Трудовым договором.

2 Университет предоставляет Работнику необходимые условия для выполнения требований по охране конфиденциальности информации, содержащей сведения конфиденциального характера Университета, к которой допускается Работник, в том числе хранилище для документов, средства для доступа к АРМ, информационным системам (ключи, пароли, персональные идентификаторы и т.п.) и др., определяемые обязанностями, выполняемыми Работником.

3 Работник разрешает Университету производить контроль использования им технических средств обработки и передачи информации, выделенных Университетом.

4 Университет оставляет за собой право, но не принимает каких-либо обязательств контролировать надлежащие использование Работником технических средств обработки и хранения информации, соблюдение им мер по охране конфиденциальности информации, содержащей сведения конфиденциального характера Университета.

5 Работнику известно, что разглашение информации, содержащей сведения конфиденциального характера Университета, ставшей ему известном в период действия Трудового договора, заключенного с Университетом, может повлечь дисциплинарную, материальную, административную, гражданско-правовую, уголовную ответственность, предусмотренную действующим законодательством Российской Федерации.

6 Работник обязуется не разглашать информацию, содержащую сведения конфиденциального характера Университета, доступ к которой получен им в связи с исполнением трудовых обязанностей, в течение всего срока действия Трудового договора, в т.ч. после прекращения трудовых отношений с Работником, до момента получения письменного уведомления от Университета о снятии режима защиты с указанной информации.

Настоящее Соглашение является неотъемлемой частью Трудового договора ' от «___»_____ 20__ г.

Подписи сторон:
Работник:
Подпись _____ /И.О.Фамилия _____
«___»_____ 20__ г.
Работодатель:
Подпись _____ /И.О.Фамилия _____
«___»_____ 20__ г.

Я подтверждаю факт получения на руки второго идентичного экземпляра Соглашения

Подпись Работника/И.О.Фамилия Работника _____

Принято решением Ученого Совета
(протокол от 25 ноября 2020 г. № 12)