Министерство образования и науки
Российской Федерации
Читинский институт (филиал)
федерального государственного
бюджетного образовательного учреждения
высшего образования
«Байкальский государственный
университет»
(ЧИ ФГБОУ ВО «БГУ»)

УТВЕРЖДАЮ
Директор ЧИ ФГБОУ ВО «БГУ»
_____Т.Д. Макаренко
«__» _____ 20__ г.

ПОЛИТИКА
информационной безопасности

ПРИНЯТО
Советом Института
Протокол № __1__
«__18__» _сентября_ 20__16__ г.

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее – Политика) разработана в соответствии с законодательством Российской Федерации в части обеспечения информационной безопасности – в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных и других правовых актов.

1.2. Настоящая Политика является локальным нормативным актом Читинского института (филиала) федерального государственного бюджетного образовательного учреждения высшего образования «Байкальский государственный университет» (далее – Института), представляет собой официально принятую систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности.

1.3. Политика является методологической основой для формирования и проведения единой политики в области обеспечения безопасности информации; принятия управленческих решений и разработке практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации; разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации.

1.4. При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

2. Объекты системы информационной безопасности

2.1. Объектами системы информационной безопасности являются:

– информационные ресурсы с ограниченным доступом, составляющие служебную, коммерческую тайну, персональные данные сотрудников или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы;

– процессы обработки информации в автоматизированной системе управления высшим учебным заведением (далее – АСУ «ВУЗ») информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

– информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены элементы информационной среды.

3. Основные угрозы безопасности информации

3.1. Все множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

3.2. Естественные угрозы – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека. Искусственные угрозы – это угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно

выделить: непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.; преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников). Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

3.3. Основными источниками угроз безопасности информации являются:

– непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия пользователей информационной системы (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;

– преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т.п.) действия легально допущенных к информационным ресурсам пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы;

– деятельность преступных групп и формирований, политических и экономических структур, разведок иностранных государств, а также отдельных лиц по добыванию информации, навязыванию ложной информации, нарушению работоспособности информационной системы в целом и ее отдельных компонентов;

– удаленное несанкционированное вмешательство посторонних лиц из территориально удаленных сегментов корпоративной информационной системы и внешних информационно-

телекоммуникационных сетей общего пользования (прежде всего сеть Интернет) через легальные и несанкционированные каналы подключения к таким сетям, используя недостатки протоколов обмена, средств защиты и разграничения удаленного доступа к ресурсам;

– ошибки, допущенные при разработке компонентов информационной системы и их систем защиты, ошибки в программном обеспечении, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты);

– аварии, стихийные бедствия.

3.4. Наиболее значимыми угрозами безопасности информации для Института (способами нанесения ущерба субъектам информационных отношений) являются: нарушение конфиденциальности (разглашение, утечка) сведений, составляющих служебную тайну, а также персональных данных; нарушение функциональности компонентов информационной системы, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач; нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов.

4. Меры обеспечения информационной безопасности

4.1. Все меры обеспечения безопасности информационной системы подразделяются на: правовые (законодательные); морально-этические; технологические; организационные (административные); физические; технические (аппаратные и программные).

4.2. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы.

4.3. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не

являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека или группы лиц или в целом. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

4.4. К технологическим мерам относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений и т.п.

4.5. Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

5. Формирование политики информационной безопасности

5.1. Политика в области обеспечения безопасности информации определяет процедуры, и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила: роли и обязанности должностных лиц, отвечающие за проведение политики безопасности информации; права доступа к информации ограниченного распространения и т.д.

5.2. Политика в области обеспечения безопасности информации должна предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов; определять коалиционные и иерархические принципы и методы разделения

конфиденциальной информации и разграничения доступа к информации ограниченного распространения; выбирать программно-технические (аппаратные) средства криптозащиты, противодействия несанкционированному доступу, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

5.3. Регламентация доступа в помещения:

– чувствительные к воздействиям компоненты информационной системы должны размещаться в помещениях, оборудованных надежными замками, средствами сигнализации и находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, серверов, реквизитов доступа и т.п.);

– уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам;

– во время обработки информации ограниченного распространения в таких помещениях должен присутствовать только персонал, допущенный к работе с данной информацией;

– запрещается прием посетителей в помещениях, когда осуществляется обработка информации ограниченного распространения;

– по окончании рабочего дня, помещения в которых размещаются чувствительные компоненты информационной системы, должны, опечатываться сдаваться под охрану с включением сигнализации и с отметкой в книге приема и сдачи помещений;

– для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, металлическими шкафами или шкафами оборудованные замком.

5.4. Регламентация допуска сотрудников к использованию информационных ресурсов:

– допуск пользователей к работе с информационной системой и доступ к ее ресурсам должен быть строго регламентирован; любые

изменения состава и полномочий пользователей подсистем должны производиться установленным порядком, согласно, регламента предоставления доступа пользователей;

– уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования: каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями; расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с подразделением, ответственным за информационное сопровождение данного ресурса.

5.5. Обучение сотрудников и повышение осведомленности в вопросах информационной безопасности:

– все пользователи информационной системы должны быть ознакомлены с документами по обеспечению информационной безопасности, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации;

– пользователи информационной системы должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации;

– целью обучения сотрудников является снижение потерь (материальных, финансовых, ущерб репутации и т.д.) от угроз, связанных с незнанием или непониманием основных положений нормативно-распорядительных документов в области информационной безопасности и правил по защите информации;

– задачи повышения осведомленности в вопросах информационной безопасности – информирование сотрудников о существующих угрозах (опасностях) и проблемах информационной безопасности, которые могут возникнуть при автоматизированной обработке информации, обновление (расширение) их теоретических и практических знаний в области информационной безопасности; доведение до сотрудников основных

положений, ограничений и требований существующих нормативно-распорядительных документов; мотивация пользователей информационной системы на сознательное выполнение ими требований, ограничений и правил обеспечения информационной безопасности; выработка у сотрудников умения здраво оценивать возможные последствия своих действий (адекватно оценивать связанные с ними риски информационной безопасности); выработка у сотрудников привычек, способствующих поддержанию высокого уровня информационной безопасности; выработка у сотрудников умений (навыков) правильно и оперативно действовать при возникновении инцидентов информационной безопасности; доведение до сотрудников их обязанностей в области обеспечения информационной безопасности и степени их ответственности в случае утечки конфиденциальной информации;

– формы и методы повышения осведомленности сотрудников в области информационной безопасности – инструктаж при приеме на работу; обучение (курсы, семинары, тренинги); распространение кратких памяток.

6. Мероприятия по обеспечению информационной безопасности

6.1. Для обеспечения информационной безопасности требуется:

– обеспечить единое планирование, согласование и проведение мероприятий по информационной безопасности и защите информации в структурных подразделениях;

– организовать аттестацию объектов, помещений, рабочих мест, аппаратно-программных средств обработки информации и систем (каналов) ее передачи на соответствие нормам действующего законодательства в сфере защиты информации и персональных данных;

– организовать обучение пользователей по вопросам информационной безопасности;

– осуществлять мониторинг информации, циркулирующей в сетях, системах, на объектах и в помещениях, в т.ч. с использованием аппаратно-программных средств выявления и предотвращения утечки информации;

– принимать меры по выявлению и устранению причин и условий, способствующих возникновению инцидентов информационной безопасности;

– принимать участие в совещаниях по вопросам информационной

безопасности;

– совершенствовать аппаратно-программные средства для обеспечения информационной безопасности.

Согласовано:

Заместитель директора по учебной работе _____ / Болтовская Л.А.

Начальник отдела автоматизированных
систем управления _____ / Куклина О.К.