ПРИНЯТЫ
Объединенным советом
обучающихся СЛИ
« 31 » мая 2021 г.
протокол № 5

ПРИНЯТЫ
Ученым Советом СЛИ
« 16 » июня 2021 г.
протокол № 8

УТВЕРЖДЕНЫ
приказом директора СЛИ
« 08 » сентября 2021 г.
№ 145/О

ПОЛОЖЕНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

в Сыктывкарском лесном институте (филиале)
федерального государственного бюджетного образовательного учреждения
высшего образования «Санкт-Петербургский государственный
лесотехнический университет имени С.М. Кирова»

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛНИЯ

1) **Университет** – Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова»;

2) **СЛИ, Институт** – Сыктывкарский лесной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова»;

3) **Положение** – Положение по информационной безопасности в Сыктывкарском лесном институте (филиале) федерального государственного бюджетного учреждения высшего образования «Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова».

4) **Информационная безопасность** – состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений.

5) **Субъекты информационных отношений** – владельцы и пользователи информации и поддерживающей инфраструктуры. К поддерживающей инфраструктуре относятся не только компьютеры, но и помещения, системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и обслуживающий персонал.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Положение регламентирует вопросы информационной безопасности в СЛИ.

2.2. Настоящее Положение разработано в соответствии с:

– Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

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

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

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

– Уставом Университета;

– Положением СЛИ

и иными локальными нормативными актами СЛИ.

2.3. Информационная безопасность в современной образовательной среде в соответствии с действующим законодательством предусматривает защиту сведений и данных, относящихся к следующим группам:

– персональные данные и сведения, которые имеют отношения к обучающимся, работникам СЛИ, оцифрованные архивные документы;

– обучающие программы, базы данных, библиотеки, другая структурированная информация, применяемая для обеспечения образовательного процесса;

– защищенная законом интеллектуальная собственность.

2.5. Обеспечение информационной безопасности осуществляется по следующим направлениям:

– правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

– организационная защита – это регламентация деятельности СЛИ и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

– инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Спецификой обеспечения информационной безопасности в СЛИ является состав характерных угроз. К ним относится не только возможность хищения или повреждения данных хакерами, но также деятельность обучающихся, которые могут сознательно или ненамеренно повредить оборудование или заразить систему вредоносными программами.

3.2. Угрозам намеренного или ненамеренного воздействия могут подвергаться следующие группы объектов:

– компьютерное и другое оборудование СЛИ, в отношении которого возможны воздействия вредоносного программного обеспечения, физические и другие воздействия;

– программное обеспечение, применяемое в образовательном процессе или для работы системы;

– данные, которые хранятся на жестких дисках или портативных носителях;

– обучающиеся, которые могут подвергаться стороннему информационному воздействию;

– работники, поддерживающие работу ИТ-системы.

3.3. Угрозы информационной безопасности СЛИ могут носить непреднамеренный и преднамеренный характер.

3.4. К непреднамеренным угрозам относятся:

– аварии и чрезвычайные ситуации – затопление, отключение электроэнергии и т. д.;

– программные сбои;

– ошибки работников;

– поломки оборудования;

– сбои систем связи.

3.5. Особенностью непреднамеренных угроз является их временное воздействие. В большинстве случаев результаты их реализации достаточно эффективно и быстро устраняются подготовленными работниками.

3.6. К более опасным относятся угрозы информационной безопасности намеренного характера, результаты реализации которых, невозможно предвидеть. Намеренные угрозы могут исходить от обучающихся, работников СЛИ, хакеров. Наиболее уязвимыми являются сети с удаленным в пространстве расположением компонентов, связи между которыми легко нарушаются, что приводит к выведению системы из строя.

3.7. Существенную угрозу представляет хищение интеллектуальной собственности и нарушение авторских прав.

3.8. Внешние атаки на компьютерные сети СЛИ могут предприниматься для воздействия на сознание обучающихся с целью вовлечения их в криминальную или террористическую деятельность.

4. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

4.1. Главной целью обеспечения безопасности информации, циркулирующей в СЛИ, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационной среды СЛИ.

4.2. Основными целями обеспечения безопасности информации являются:

– предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в СЛИ;

– предотвращение нарушений прав личности обучающихся, педагогических работников и других работников СЛИ на сохранение конфиденциальности информации;

– предотвращение несанкционированных действий по блокированию информации.

4.3. Основными задачами обеспечения безопасности информации являются:

– соответствие положениям законодательных актов и нормативным требованиям по защите информации;

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам СЛИ, нарушению нормального функционирования и развития СЛИ;

– создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

– эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

– развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

– развитие и совершенствование защищенного юридически значимого электронного документооборота;

– создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;

– создание механизмов управления системой информационной безопасности.

5. ПРАВОВЫЕ НОРМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. СЛИ имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников СЛИ, требовать от своих работников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

5.2. СЛИ обязан обеспечить сохранность конфиденциальной информации.

5.3. Директор СЛИ:

– назначает ответственного за обеспечение информационной безопасности;

– имеет право включать требования по обеспечению информационной безопасности в коллективный договор;

– имеет право включать требования по защите информации в договоры по всем видам деятельности;

– разрабатывает перечень сведений конфиденциального характера;

– имеет право требовать защиты интересов СЛИ со стороны государственных и судебных инстанций.

5.4. Организационные и функциональные документы по обеспечению информационной безопасности:

– приказ директора СЛИ о назначении ответственного за обеспечение информационной безопасности;

– перечень защищаемых информационных ресурсов и баз данных;

– инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней работников СЛИ и др.

5.5. Порядок допуска работников СЛИ к информации предусматривает:

– принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;

– ознакомление работника с нормами законодательства РФ и СЛИ об информационной безопасности и ответственности за разглашение информации конфиденциального характера;

– инструктаж работника специалистом по информационной безопасности;

– контроль работника ответственным за информационную безопасность, при работе с информацией конфиденциального характера.

6. ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в СЛИ устанавливаются:

– защита интеллектуальной собственности СЛИ;

– защита компьютеров, локальных сетей и сети подключения к системе Интернет;

– организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся СЛИ;

– учет всех носителей конфиденциальной информации;

– контроль над использованием электронных средств информационного обеспечения деятельности СЛИ по прямому назначению;

– противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности СЛИ нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;

– принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;

– обучение работников СЛИ по вопросам обеспечения информационной безопасности;

– контроль за правильностью использования имеющихся в СЛИ средств телефонной и радиосвязи.

7. ОРГАНИЗАЦИЯ РАБОТЫ С ИНФОРМАЦИОННЫМИ РЕСУРСАМИ И ТЕХНОЛОГИЯМИ

7.1. Система организации делопроизводства:

– учет всей документации СЛИ, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;

– регистрация и учет всех входящих (исходящих) документов СЛИ в электронной базе данных (в специальном журнале информации) о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);

– регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);

– особый режим уничтожения документов.

7.2. В ходе использования, передачи, копирования и исполнения документов необходимо соблюдать определенные правила:

7.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.

7.2.2. Документы, дела и издания с грифом «Для служебного пользования» («Ограниченного пользования») должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах.

При этом должны быть созданы условия, обеспечивающие их физическую сохранность.

7.2.3. Выданные для работы дела и документы с грифом «Для служебного пользования» («Ограниченного пользования») подлежат возврату в канцелярию в тот же день.

7.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства структурного подразделения СЛИ.

7.2.5. Запрещается выносить документы с грифом «Для служебного пользования» за пределы СЛИ.

7.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

7.3. Все программное обеспечение устанавливается только с разрешения ответственного за информационную безопасность.

Конец документа