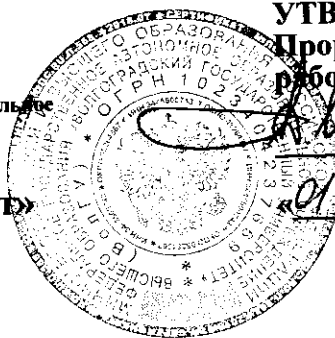




Федеральное государственное автономное образовательное учреждение высшего образования

**«Волгоградский
государственный университет»
(ВолГУ)**



УТВЕРЖДАЮ
**Проректор по учебной
работе ВолГУ**

Д.И. Ильин
Д.И. Ильин

«01» 12 2020г.

ПОЛОЖЕНИЕ
о лаборатории безопасности
сетей ЭВМ, защищенных
информационных и
автоматизированных систем
01.12.2020г. № 01-23-1766

1. Общие положения

1.1. Лаборатория безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем (аудитория 2-246, корпуса К) является направлением деятельности кафедры информационной безопасности института приоритетных технологий федерального государственного автономного образовательного учреждения высшего образования «Волгоградский государственный университет» и обеспечивает выполнение лабораторных работ при подготовке студентов по направлениям подготовки специалистов 10.05.03 «Информационная безопасность автоматизированных систем», 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», бакалавров 10.03.01 «Информационная безопасность», магистров 10.04.01 «Информационная безопасность», а также выполнение работ инновационного студенческого конструкторского бюро (далее СКБ).

1.2. Руководство лабораторией безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем осуществляет заведующий кафедрой информационной безопасности.

1.3. Заведующий кафедрой и руководитель СКБ в соответствии с должностными инструкциями осуществляют организацию и руководство всеми видами деятельности лаборатории и несут полную ответственность за результаты их работы.

2. Цели и задачи

2.1. Цель:

Формирование у обучающихся практических навыков для будущей профессиональной деятельности в соответствии с формируемыми компетенциями по направлениям подготовки:

а) бакалавров 10.03.01 «Информационная безопасность»:

-ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;

-ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

-ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

Название документа: Положение о лаборатории безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем

Разработчик: И.о. заведующего кафедрой информационной безопасности Какорина О.А. Страница 1 из 8

Версия 1

Копии с данного оригинала при распечатке недействительны без заверительной надписи

-ОПК-6: способность применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;

-ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

-ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

-ПК-3: способность администрировать подсистемы информационной безопасности объекта защиты;

-ПК-5: способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;

-ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

-ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;

-ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;

-ПК-12: способность принимать участие в проведении экспериментальных исследований системы защиты информации;

-ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

б) специалистов 10.05.03 «Информационная безопасность автоматизированных систем»:

-ОПК-2: способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники;

-ОПК-3: способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности;

-ОПК-5: способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

-ОПК-6: способность применять нормативные правовые акты в профессиональной деятельности;

-ОПК-8: способность к освоению новых образцов программных, технических средств и информационных технологий;

-ПК-2: способность создавать и исследовать модели автоматизированных систем;

-ПК-3: способность проводить анализ защищенности автоматизированных систем;

Название документа: Положение о лаборатории безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем
Разработчик: И.о. заведующего кафедрой информационной безопасности Какорина О.А. Страница 2 из 8
Версия 1
Копии с данного оригинала при распечатке недействительны без заверительной надписи

- ПК-4: способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;
 - ПК-5: способность проводить анализ рисков информационной безопасности автоматизированной системы;
 - ПК-6: способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;
 - ПК-8: способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;
 - ПК-9: способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;
 - ПК-11: способность разрабатывать политику информационной безопасности автоматизированной системы;
 - ПК-12: способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;
 - ПК-13: способность участвовать в проектировании средств защиты информации автоматизированной системы;
 - ПК-15: способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем;
 - ПК-16: способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;
 - ПК-17: способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
 - ПК-19: способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;
 - ПК-20: способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;
 - ПК-21: способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;
 - ПК-22: способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;
 - ПК-23: способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;
 - ПК-24: способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;
 - ПК-25: способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
 - ПК-26: способность администрировать подсистему информационной безопасности автоматизированной системы;
 - ПК-27: способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы;
 - ПК-28: способность управлять информационной безопасностью автоматизированной системы;
- в) специалистов 10.05.05 «Безопасность информационных технологий в

правоохранительной сфере»:

-ОПК-1: способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач;

-ОПК-2: способность проводить мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств обработки и защиты информации;

-ПК-1: способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз;

-ПК-6: способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации;

-ПК-8: способность участвовать в выявлении, предупреждении, пресечении, раскрытии и расследовании преступлений в качестве специалиста, реализовывать мероприятия по получению информации, анализировать, оценивать ее и эффективно использовать в интересах выявления, предупреждения, пресечения, раскрытия и расследования преступлений;

-ПК-10: способность правильно и полно отражать результаты профессиональной деятельности в служебной документации;

-ПК-13: способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;

-ПК-17: способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов;

-ПК-18: способность разрабатывать предложения по совершенствованию системы управления безопасностью информации;

-ПК-19: способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности;

-ПК-20: способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач;

-ПК-21: способность формировать и поддерживать в актуальном состоянии автоматизированные базы и банки данных, использовать информационно-поисковые и логико-аналитические системы;

-ПК-22: способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности;

-ПК-23: способность применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ, идентификацию, диагностику, прогнозирование; криминалистическую диагностику;

-ПК-25: способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования;

Название документа: Положение о лаборатории безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем

Разработчик: И.о. заведующего кафедрой информационной безопасности Какорина О.А. Страница 4 из 8

Версия 1

Копии с данного оригинала при распечатке недействительны без заверительной надписи

- ПК-26: способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты;
- ПК-27: способность готовить научные отчеты по результатам выполненных исследований;
- ПК-28: способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны;
- ПК-29: способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации;
- ПК-30: способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации;
- ПК-31: способность принимать участие в создании системы защиты информации на объекте информатизации;
- г) магистров 10.04.01 «Информационная безопасность»:
- ОПК-1: способность к коммуникации в устной и письменной формах на государственном и одном из иностранных языков для решения задач профессиональной деятельности;
- ОПК-2: способность к самостоятельному обучению и применению новых методов исследования профессиональной деятельности;
- ПК-1: способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;
- ПК-2: способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;
- ПК-3: способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;
- ПК-4: способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности;
- ПК-6: способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;
- ПК-7: способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента;
- ПК-8: способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;
- ПК-9: способность проводить аудит информационной безопасности информационных систем и объектов информатизации;
- ПК-10: способность проводить аттестацию объектов информатизации по требованиям безопасности информации;
- ПК-13: способность организовать управление информационной безопасностью;
- ПК-14: способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с

правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

-ПК-15: способность организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

-ПК-16: способность разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

2.2. Для реализации данных целей лабораторией безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем решаются следующие задачи:

а) проведение аудиторных лабораторных занятий, учебных практик, курсовых и выпускных квалификационных работ, предусмотренных учебным планом по направлениям подготовки специалистов 10.05.03 «Информационная безопасность автоматизированных систем» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», бакалавров 10.03.01 «Информационная безопасность», магистров 10.04.01 «Информационная безопасность»;

б) осуществление индивидуальной подготовки студентов к занятиям и консультативной работы с ними преподавателей кафедры;

в) проведение тренингов и консультаций для студентов;

г) централизованное хранение, выдача и разработка учебно-методических материалов;

д) обеспечение научно-исследовательской работы кафедры информационной безопасности;

е) проведение профессиональной ориентационной работы кафедры информационной безопасности.

2.3. Материально-техническое обеспечение лаборатории:

-12 рабочих комплексов, программно-аппаратный комплекс "Соболь" с электронным идентификатором iButton DS1992 в комплекте ПАК (3 шт.), Secret Net клиент 7 и 8 (по 10 лицензий), комплекс "Сетевое оборудование "Cisco" часть 1, СКАНЕР-ВС (10 лицензий), РУБИКОН-К (10 лицензий).

2.4. Обеспечение инновационной научной деятельности СКВ.

3. Процессы и функции

3.1. Лаборатория безопасности сетей ЭВМ и защищенных информационных и автоматизированных систем в рамках процесса «Организация и реализация основных образовательных программ» осуществляет следующие функции:

а) проводятся лабораторные занятия, предусмотренные учебным планом по направлениям подготовки специалистов 10.05.03 «Информационная безопасность автоматизированных систем» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», бакалавров 10.03.01 «Информационная безопасность», магистров 10.04.01 «Информационная безопасность»;

б) осуществляется организация и контроль самостоятельной работы студентов;

в) осуществляется комплексное методическое обеспечение учебных дисциплин кафедры информационной безопасности;

г) осуществляется эффективное использование имеющейся современной вычислительной техники, программного обеспечения и лабораторного оборудования.

3.2. Лаборатория безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем в рамках процесса «Управление НИР» осуществляет следующие функции:

а) принимается участие в подготовке и проведении конференций, семинаров,

Название документа: Положение о лаборатории безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем

Разработчик: И.о. заведующего кафедрой информационной безопасности Какорина О.А. Страница 6 из 8

Версия 1

Копии с данного оригинала при распечатке недействительны без заверительной подписи

совещаний по проблемам профессиональной подготовки специалистов по направлениям подготовки 10.05.03 «Информационная безопасность автоматизированных систем» и 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», направлениям подготовки бакалавров 10.03.01 «Информационная безопасность», магистров 10.04.01 «Информационная безопасность»;

б) создаются условия для активного привлечения студентов к научным исследованиям, осуществляемым кафедрой информационной безопасности;

в) проводится работа по развитию, модернизации и укреплению материально-технической базы кафедры, включая постоянное совершенствование учебно-методического оборудования, оснащения кафедры современными вычислительными и программными средствами и их широкое внедрение в учебный процесс;

г) принимается участие в научно-исследовательской работе кафедры информационной безопасности.

3.3. Лаборатория безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем в рамках процесса «Обеспечение деятельности СКВ» осуществляет следующие функции:

а) оказывает консультативную помощь малым фирмам по вопросам внедрения и использования информационных технологий, защиты информации и работе с персональными данными;

б) осуществляет повышение квалификации и обучение сотрудников малого бизнеса;

в) проводит информационно-ресурсное обеспечение процессов внедрения новых технологий.

4. Ответственность и полномочия

4.1. Сотрудники, работающие в лаборатории безопасности сетей ЭВМ и защищенных информационных и автоматизированных систем, имеют право:

а) на участие в планировании учебной, учебно-методической и научно-исследовательской работы кафедры информационной безопасности;

б) на использование в своей работе учебных, методических и научных разработок преподавателей кафедры по согласованию с ними;

в) на создание необходимых условий использовать информационное и материальное обеспечение для профессиональной деятельности.

4.2. Текущая исполнительская деятельность осуществляется лаборантом кафедры.

Лаборант:

- проводит инструктаж по безопасности труда и пожарной безопасности на рабочем месте;

- контролирует выполнение обучающимися правил безопасности труда и пожарной безопасности;

- сопровождает лабораторные работы согласно утвержденному расписанию проведения занятий, курсовые и выпускные квалификационные работы, выполняемые в соответствии с учебным планом по утвержденному графику работы;

- несет ответственность за выполнение планов работы, сохранность оборудования и материалов, четкое выполнение должностных обязанностей;

- имеет право отказать в возможности работать в лаборатории за грубое нарушение правил безопасности труда и пожарной безопасности до внеочередного прохождения инструктажа.

Сотрудники, работающие в лаборатории безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем, обязаны:

Название документа: Положение о лаборатории безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем

Разработчик: И.о. заведующего кафедрой информационной безопасности Какорина О.А. Страница 7 из 8

Версия 1

Копии с данного оригинала при распечатке недействительны без заверительной надписи

а) эффективно использовать свой учебно-методический потенциал для осуществления закрепленных функций, развивать и качественно улучшать его через привлечение к работе всех преподавателей кафедры информационной безопасности;

б) содействовать внедрению в учебный процесс современных эффективных образовательных, педагогических, научно-исследовательских технологий при осуществлении своих функций.

в) содействовать вовлечению студентов и аспирантов в практическую реализацию инновационных проектов, выполняемых в рамках СКБ.

4.3. В текущей работе сотрудники, выполняющие работы в лаборатории безопасности сетей ЭВМ и защищенных автоматизированных систем, руководствуются приказами ректора ВолГУ, распоряжениями директора института приоритетных технологий, уставными документами СКБ и другими внешними и внутренними документами, регламентирующими деятельность кафедры и СКБ.

4.4. Сотрудники кафедры, выполняющие работы в лаборатории безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем, несут ответственность за:

- а) неисполнение или ненадлежащее исполнение своих должностных обязанностей;
- б) правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством РФ;
- в) причинение материального ущерба в пределах, определенных действующим трудовым и гражданским законодательством РФ.

5. Взаимоотношения

5.1. Лаборатория безопасности сетей ЭВМ, защищенных информационных и автоматизированных систем включается в состав кафедры информационной безопасности, действует в рамках плана работы кафедры и исполняет распоряжения заведующего кафедрой и руководителя СКБ.

И.о. заведующего кафедрой
информационной безопасности

О.А. Какорина

СОГЛАСОВАНО

И.о. директора института
приоритетных технологий

С.В. Борознин

Начальник УОП

Л.Н. Канищева

Начальник УД
17.11.20

И.В. Манаенков

Начальник общего отдела

Н.С. Станкевич