МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Горский государственный аграрный университет»

«УТВЕРЖДАЮ»
Ректор ФГБОУ ВО
Горский ГАУ
_____О.К. Гогаев
«_12_» _01._ 2024г.

ФАКУЛЬТЕТ

ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ КАДРОВ

ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Программа	**«Основы кибербезопасности»**
Форма обучения	**– очно-заочная**
Базовое образование	**– среднее профессиональное, высшее**
Срок обучения	**– 72 часа**

ВЛАДИКАВКАЗ - 2024

Общая информация

Повышение квалификации по курсу «Основы кибербезопасности» представляет собой дополнительное профессиональное образование в виде обучения лиц, имеющих неполное высшее или высшее образование. Продолжительность обучения составляет две недели, объем 72 учебных часа. Форма контроля – зачет.

Программа повышения квалификации предусматривает проведение занятий в традиционной форме (лекции, лабораторно-практические занятия). Она реализуется с использованием дистанционных образовательных технологий. Изучение нового материала носит сопровождающий характер. Для отработки навыков и умений предусмотрены тренировочные задания, которые предполагают овладение общими принципами работы. Затем следует углубление знаний и практическое применение средств и возможностей прикладного программного обеспечения и теоретического материала.

По окончании курса слушателям выдается удостоверение установленного образца о повышения квалификации в объеме 72 учебных часов.

Актуальность создания программы

Разработка данной программы продиктована необходимостью формирования у обучающихся новых знаний в области нормативно-правовых основ информационной безопасности в РФ и умений выбирать стандарты и механизмы кибербезопасности для защиты распределенных систем.

Цель реализации программы

Целью данной программы является формирование и развитие следующих знаний и умений:

- подготовить слушателей к практической деятельности: уметь использовать методы и приемы, используемые для обнаружения различных видов уязвимостей;
- сформировать прочные знания по курсу, а также качественно улучшить имевшиеся ранее;
- привить творческий подход и навыки самостоятельной работы с методами и средствами сбора информации и ее хранения, источниками распространения информации об уязвимостях, техниках получения несанкционированного доступа;

- сформировать навыки о методиках прогнозирования и/или эмуляции угроз, примерах использования системных артефактов в компьютерной профилактике угроз кибербезопасности и т.д.

Содержание

Раздел 1. Комплексная защита и хранение информации в компьютерных системах. Предупреждение незаконных действий в отношении компьютерной информации (20 часов).

Ознакомление слушателей с этапами развития информационных технологий, тенденциями и проблемами их развития. Негативные аспекты информатизации и компьютеризации современного общества. Понятие и принципы информационного обеспечения. Информационные системы, состояние и перспективы информатизации компьютерных систем.

Понятие информационной безопасности и защиты информации. Угрозы и риски в работе компьютерных систем. Государственные органы в сфере защиты информации. Методы защиты информации. Противоправные действия в информационной сфере.

Предупреждение незаконных действий в отношении компьютерной информации. Организационные основы защиты информации и обеспечение кибербезопасности. Понятие допуска к информации. Электронное конфиденциальное делопроизводство. Архивирование и уничтожение конфиденциальных источников информации.

Слушатели должны знать:

- основные понятия и принципы информационного обеспечения компьютерных систем;
- понятие допуска к информации;

Слушатели должны уметь:

- оценивать угрозы и риски в информационной сфере и применять информационные системы в бытовой и профессиональной деятельности;
- осуществлять процедуру оформления прав на доступ к защищаемой информации;

Слушатели должны владеть:

- навыками анализа состояния и перспектив информатизации в бытовой и профессиональной сфере;

- навыками организационных подходов к обеспечению защиты информации и выстраиванию системы кибербезопасности;
- навыками применения процедуры оформления прав на проведение работ с использованием защищаемой информации;

Во время изучения данного раздела слушатели выполняют следующие задания:

Изучить процедуры оформления права на доступ к защищаемой информации.

Ознакомиться с процедурами оформления прав на проведение работ с использованием защищаемой информации.

Идентификация и аутентификация пользователей.

Дискреционное разграничение доступа.

Мандатное разграничение доступа.

Ролевое разграничение доступа.

Работа с БД в среде табличного процессора Microsoft Excel. Защита информации в Excel. Реализация шифра Цезаря в Microsoft Excel.

Раздел 2. Математические основы криптографии. Эволюция симметричного шифрования. (16 часов)

Цель изучения раздела – дать знания в области криптографической защиты информации, доступно изложить математический аппарат криптографии, не прибегая к полным доказательствам теорем, приводя лишь их схемы.

Математические основы криптографии. Эволюция симметричного шифрования. Элементы криптоанализа классических шифров.

Основы ассиметричного шифрования. Идентификация и аутентификация. Управление криптографическими ключами. Электронная подпись.

Слушатели должны знать:

- теоретические основы организации конфиденциального делопроизводства для обеспечения защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и других неправомерных действий в отношении информации;

Слушатели должны уметь:

- применять основы электронного конфиденциального делопроизводства и шифрования;

Слушатели должны владеть:

- навыками архивирования и уничтожения конфиденциальных носителей информации;

Изучение данного раздела расширяет представление слушателей о сути криптографических алгоритмов через общие понятия и методы базовых математических преобразований.

Во время изучения данного раздела слушатели выполняют практические задания:

Метод простых замен. Шифрование (дешифрование).
Метод перестановок. Шифрование (дешифрование).
Метод сложных замен. Шифрование (дешифрование).
Программная реализация алгоритмов электронной цифровой подписи.

Раздел 3. Основы государственной политики Российской Федерации в области информационной безопасности. (18 часов)

Изучение раздела способствует повышению знаний слушателей по основным вопросам юридической ответственности за нарушение законодательства Российской Федерации в области информационной безопасности.

Понятие и правовая сущность информационной безопасности РФ. Информационная безопасность как составная часть национальной безопасности. Доктрина информационной безопасности РФ 2016г. Внутренние и внешние информационные угрозы. Основные направления обеспечения информационной безопасности современного российского государства 1) защита информационных прав и свобод человека и гражданина, 2) защита информационных ресурсов от неправомерного доступа, 3) защита общества от вредной и недоброкачественной информации.

Киберпреступность как основная угроза информационной безопасности. Уголовная, административная, гражданско-правовая и дисциплинарная ответственность за нарушение законодательства в области информационной безопасности.

Правовое просвещение и правовое информирование населения как способ борьбы с кибермошенничеством.

Слушатели должны знать:

- нормативные правовые акты, регламентирующие оборот информации;
- виды киберпреступлений;
- виды ответственности за правонарушения в сфере информации, информационных технологий и защиты информации.

Слушатели должны уметь:

- анализировать и применять нормативно-правовые акты в сфере защиты информации в различных сферах деятельности;
- анализировать специфику кибермошенничества.

Слушатели должны владеть:

- юридической терминологией в области информационной безопасности и киберпреступности;
- навыками решения задачи определения вида ответственности за правонарушения в сфере информации, информационных технологий и защиты информации.

Раздел 4. Угрозы и риски внедрения новых финансовых технологий в банковской сфере. (18 часов)

Изучение раздела формирует у слушателей понимание ландшафта банковских информационных технологий, архитектуры банковских информационных систем и знакомит с основными тенденциями и рисками в области информационной безопасности в финансовой сфере.

Понятие инновации и технологии. Классификация технологий. Инновационные решения и новые тенденции в сфере современных банковских технологий. Перспективные финансовые технологии. Анализ практики внедрения финансовых технологий в банковской сфере.

Проблематика безопасности в банковской сфере. Основы финтех-индустрии. Сферы применения открытого банкинга и анализ безопасности Open API. Кибермошенничество и социальная инженерия. Проблемы уязвимости банковских мобильных приложений. Анализ безопасности готовых приложений банк-клиент. Обеспечение безопасности и устойчивости применения финансовых технологий в банковской сфере.

Слушатели должны знать:

- состав защищаемых информационных ресурсов в банковской сфере;
- характеристики основных режимов использования отдельных видов информационных ресурсов, в том числе в финансовой области.

Слушатели должны уметь:

- использовать информацию, относящуюся к государственной тайне, служебной тайне, иной конфиденциальной информации;
- применять инструменты функционирования режимов различных видов профессиональных тайн в банковской сфере.

Слушатели должны владеть:

- навыками решения задачи использования информации как объекта публичных, гражданских или иных отношений;
- навыками решения задач по обеспечению функционирования режимов защиты государственной и служебной тайны, персональных данных, коммерческой тайны.

Во время изучения раздела слушатели выполняют практические задания:

– Проанализировать организационные меры по защите банковских информационных систем.
– Охарактеризовать программно-технические меры организации защиты банковских информационных систем.
– Охарактеризовать такую угрозу, как «криптовымогатели».
– Объяснить сущность понятия «социальная инженерия».
– Проблемы внедрения биометрической системы удалённой идентификации клиентов.
– Анализ доступных в настоящее время методов безопасности.

Ведущие преподаватели

В учебном процессе принимают участие доценты, кандидаты наук:

Фидарова Светлана Израильевна – проректор по учебной работе и цифровизации, кандидат экономических наук, доцент.

Алборова Светлана Заурбековна – заведующий кафедрой естественнонаучных дисциплин, кандидат педагогических наук, доцент.

Датиева Мадина Черменовна – заведующий кафедрой информационных технологий, кандидат экономических наук, доцент .

Езеева Ирина Руслановна – кандидат экономических наук, доцент кафедры менеджмента.

Гогаева Альбина Леонидовна – кандидат юридических наук, доцент кафедры конституционного и административного права.

Учебный план
программы повышения квалификации
«Основы кибербезопасности»

Категория слушателей – студенты и преподаватели университета.

Объем обучения – 72 часа.

Форма обучения – очно-заочная.

Форма контроля – зачёт.

Всего учебным планом предусмотрено изучение четырёх разделов по курсу «Основы кибербезопасности», по каждой из которых сдаются зачёты. Из общего объёма 72 часов, предусмотренных учебным планом, 47% отведено для лекционных и практических занятий и 53% на самостоятельную работу.

№ п/п	Наименование разделов	Всего часов	В том числе			Форма контроля
			лекции	практические занятия	самостоятельная работа	
1.	Комплексная защита и хранение информации в компьютерных системах. Предупреждение незаконных действий в отношении компьютерной информации.	20	6	4	10	Зачёт
2.	Математические основы криптографии. Эволюция симметричного шифрования.	16	4	4	8	Зачёт
3.	Основы государственной политики Российской Федерации в области информационной безопасности.	18	4	4	10	Зачёт
4.	Угрозы и риски внедрения новых финансовых технологий в банковской сфере.	18	4	4	10	Зачёт
	ИТОГО:	**72**	**18**	**16**	**38**	

Материально-технические условия реализации программы

Организационные условия реализации разделов программы повышения квалификации осуществляются на основе общих требований к условиям реализации курсов повышения квалификации. Занятия проходят в здании факультета экономики и менеджмента.

Наименование специализированных аудиторий, кабинетов	Вид занятий	Наименование оборудования, программного обеспечения
Учебная аудитория для проведения занятий лекционного и семинарского типа (Пом. № 2.1.06.)	лекции	мебель, доска настенная, рабочее место преподавателя, комплект мультимедийного оборудования, экран-доска.
Компьютерный класс для проведения практических занятий (Пом. № 2.3.07)	практические занятия	компьютеры, интерактивная панель, специализированная мебель, рабочее место преподавателя

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Бабаш, А. В., Криптографические методы защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2024. — 189 с. — ISBN 978-5-406-11913-6. — URL: https://book.ru/book/949929 — Текст : электронный.
2. Чернова, О. А., Основы документооборота и режима секретности.: учебник / О. А. Чернова. — Москва : КноРус, 2023. — 263 с. — ISBN 978-5-406-10683-9. — URL: https://book.ru/book/946261 — Текст : электронный.
3. Банковские информационные системы и технологии : учебник / О. И. Лаврушин, В. И. Соловьев, В. Е. Косарев [и др.] ; под ред. О. И. Лаврушина, В. И. Соловьева. — Москва : КноРус, 2023. — 527 с. — ISBN 978-5-406-10982-3. — URL: https://book.ru/book/94713 — Текст : электронный.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

4. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ // Информационно-правовой портал «Гарант» http://www.garant.ru
5. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации // "Информационно-правовой портал «Гарант» http://www.garant.ru/
6. Фатьянов, А.А. Основные правовые системы ограничения в доступе к информации в Российской Федерации. Первичные системы : монография / Фатьянов А.А. — Москва : КноРус, 2020. — 210 с. — ISBN 978-5-406-07659-0. — URL: https://book.ru/book/935694.
7. Верещагина, Е. А., Исследование проблем информационной безопасности в банковской сфере : монография / Е. А. Верещагина, А. Л. Золкин, А. В. Фролов. — Москва : Русайнс, 2023. — 177 с. — ISBN 978-5-466-03976-4. — URL:

https://book.ru/book/950915 — Текст : электронный.
8. Рудакова, О. С., Финансовые технологии в банках : учебник / О. С. Рудакова, О. М. Маркова, Н. Н. Мартыненко, ; под ред. О. С. Рудаковой. — Москва : КноРус, 2024. — 309 с. — ISBN 978-5-406-12219-8. — URL: https://book.ru/book/950746 — Текст : электронный.
9. Носова, С. С., Искусственный интеллект и экономика : учебник / С. С. Носова, А. Н. Норкина. — Москва : КноРус, 2024. — 399 с. — ISBN 978-5-406-12642-4. — URL: https://book.ru/book/951959 — Текст : электронный.
10. Прокофьев, С. Е., Основы защиты информации в системе государственного и муниципального управления (с практикумом) : учебник / С. Е. Прокофьев, Р. Е. Артюхин, О. В. Панина, К. Е. Лукичев. — Москва : КноРус, 2022. — 215 с. — ISBN 978-5-406-09475-4. — URL: https://book.ru/book/943134 — Текст : электронный.
11. Литвиненко, В. И., Основы информационной безопасности : учебное пособие / В. И. Литвиненко, Е. С. Козлов. — Москва : КноРус, 2022. — 199 с. — ISBN 978-5-406-09438-9. — URL: https://book.ru/book/943111 — Текст : электронный.
12. Максуров, А. А., Защита оборота персональных данных в киберпространстве : монография / А. А. Максуров. — Москва : Русайнс, 2023. — 123 с. — ISBN 978-5-466-03765-4. — URL: https://book.ru/book/950903 — Текст : электронный.
13. Подсобляева, О. В. Безопасность информационных систем и баз данных : учебное пособие / О. В. Подсобляева. — 2-е изд., стер. — Москва : ФЛИНТА, 2022. — 99 с. — ISBN 978-5-9765-5148-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/266405 — Режим доступа: для авториз. пользователей.
14. Информационные технологии и базы данных в экономике : учебное пособие / составители Л. В. Климкина [и др.]. — пос. Караваево : КГСХА, 2018. — 45 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133557 — Режим доступа: для авториз. пользователей.

Составители:

Заведующий кафедрой информационных технологий, доцент _____ М.Ч. Датиева

Доцент кафедры менеджмента _____ И.Р. Езеева

Согласовано:

Проректор по учебной работе и цифровизации, доцент _____ С.И. Фидарова

Проректор по дополнительному образованию, профессор _____ А.Г. Ваниев

Специалист по УМР _____ Н.В. Туаева