Министерство сельского хозяйства Российской Федерации
Департамент научно-технологической политики и образования
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Красноярский государственный аграрный университет»

Институт Экономики и финансов АПК
Кафедра «Бизнес информатика и информационно-компьютерная безопасность»

СОГЛАСОВАНО:
Директор института _____ Озерова М.Г.
"23" 09 2014 г.

УТВЕРЖДАЮ
Ректор _____ Пугленок Н.В.
"___" 09 2014 г.

ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Б5.П.1 «Практика на электронных вычислительных машинах: информационные технологии, техническая защита информации»

для подготовки бакалавров
ФГОС ВПО
Направление 090900.62 «Информационная безопасность»

Профиль Информационно-аналитические системы финансового мониторинга
Курс 3
Семестры 6
Форма обучения очная
Квалификация выпускника бакалавр

Красноярск 2014

Составитель: Филиппов К.А., доктор физико-математических наук, доцент
_____ «10» ____09____ 2014 г.

Программа разработана в соответствии с ФГОС ВО по направлению подготовки 01.03.02 «Прикладная математика и информатика»

Программа обсуждена на заседании кафедры протокол
№ ____1____ «13» ____09____ 2014 г.

Зав. кафедрой Богульская Н.А.,кандидат физико-математических наук, доцент
_____ «13» ____09____ 2014 г.

Программа одобрена методической комиссией института Экономики и финансов АПК протокол № ____1____ «23» ____09____ 2014 г.

Директор института
ОзероваМ.Г., к.э.н., доцент _____ «23» ____09____ 2014 г.

Аннотация.

Целью прохождения производственной практики является изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или корпораций; приобретение навыков практического решения задач защиты информации на рабочем месте.

Задачи практики:

−углубление знаний, полученных в ходе обучения, развитие навыков их применения в практической области защиты информации;

−расширение представлений о функциональных возможностях защищенных информационных систем;

−усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;

−сбор материала для последующего его использования при изучении учебных дисциплин;

−углубление практических умений и навыков по профессиональной деятельности в рамках направления "Информационная безопасность";

−формирование умения анализировать и оценивать свою собственную профессиональную деятельность.

Процесс прохождения практики направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО и ООП ВПО по данному направлению подготовки:

а) общекультурные (ОК):

ОК-5 способностью к кооперации с коллегами, работе в коллективе;

ОК-6 способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7 способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

ОК-8 способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9 способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11 способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12 способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков.

б) профессиональные (ПК):

ПК-1 способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-3 способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-4 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

ПК-5 способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых

задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-8 способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;

ПК-9 способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

ПК-10 способностью администрировать подсистемы информационной безопасности объекта;

ПК-11 способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-12 способностью участвовать в разработке подсистемы управления информационной безопасностью;

ПК-13 способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-14 способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-15 способностью применять программные средства системного, прикладного и специального назначения;

ПК-16 способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-19 способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20 способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-24 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-28 способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;

ПК-29 способностью участвовать в работах по реализации политики информационной безопасности;

ПК-32 способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

В результате прохождения данной практики обучающийся должен приобрести следующие практические навыки и умения:

- знать:

1) права и обязанности человека и гражданина,
2) теоретический и практический материал по базовым дисциплинам;
3) методы организации и ведения рабочего процесса;

- уметь:

1) применять современные методы организации и ведения рабочего процесса в организации;
2) использовать в социальной, познавательной и профессиональной деятельности навыки работы с персональным компьютером, программным обеспечением и сетевыми ресурсами, пользоваться базами данных;
3) пользоваться в процессе работы знаниями в области ИКТ;

4) использовать на практике методы гуманитарных, социальных и экономических наук в различных видах профессиональной и социальной деятельности;

- владеть:

способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности.

Цели и задачи производственной практики. Компетенции, формируемые в результате освоения.

Целью прохождения производственной практики является изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или корпораций; приобретение навыков практического решения задач защиты информации на рабочем месте.

Задачи практики:

−углубление знаний, полученных в ходе обучения, развитие навыков их применения в практической области защиты информации;

−расширение представлений о функциональных возможностях защищенных информационных систем;

−усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;

−сбор материала для последующего его использования при изучении учебных дисциплин;

−углубление практических умений и навыков по профессиональной деятельности в рамках направления "Информационная безопасность";

−формирование умения анализировать и оценивать свою собственную профессиональную деятельность.

Процесс прохождения практики направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО и ОПОП ВПО по данному направлению подготовки:

а) общекультурные (ОК):

ОК-5 способностью к кооперации с коллегами, работе в коллективе;

ОК-6 способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;

ОК-7 способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;

ОК-8 способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения, владеть культурой мышления;

ОК-9 способностью логически верно, аргументированно и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;

ОК-11 способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;

ОК-12 способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков.

б) профессиональные (ПК):

ПК-1 способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;

ПК-3 способностью использовать нормативные правовые документы в своей профессиональной деятельности;

ПК-4 способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

ПК-5 способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых

задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

ПК-8 способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;

ПК-9 способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;

ПК-10 способностью администрировать подсистемы информационной безопасности объекта;

ПК-11 способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

ПК-12 способностью участвовать в разработке подсистемы управления информационной безопасностью;

ПК-13 способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-14 способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;

ПК-15 способностью применять программные средства системного, прикладного и специального назначения;

ПК-16 способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;

ПК-19 способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;

ПК-20 способностью применять методы анализа изучаемых явлений, процессов и проектных решений;

ПК-24 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

ПК-28 способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;

ПК-29 способностью участвовать в работах по реализации политики информационной безопасности;

ПК-32 способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;

В результате прохождения данной практики обучающийся должен приобрести следующие практические навыки и умения:

- знать:

4) права и обязанности человека и гражданина,
5) теоретический и практический материал по базовым дисциплинам;
6) методы организации и ведения рабочего процесса;

- уметь:

5) применять современные методы организации и ведения рабочего процесса в организации;
6) использовать в социальной, познавательной и профессиональной деятельности навыки работы с персональным компьютером, программным обеспечением и сетевыми ресурсами, пользоваться базами данных;
7) пользоваться в процессе работы знаниями в области ИКТ;

8) использовать на практике методы гуманитарных, социальных и экономических наук в различных видах профессиональной и социальной деятельности;

- владеть:

1) способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности

Место производственной практики в структуре ООП

Производственная практика «Практика на электронных вычислительных машинах: информационные технологии, техническая защита информации» предполагает знакомство студентов с такими учебными дисциплинами, как «Информатика», «Лицензирование и сертификация системы защиты информации», «Основы информационной безопасности», «Программно-аппаратные средства защиты информации», «Криптографические методы защиты информации», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации», «Управление информационной безопасностью», «Принципы построения, проектирования и эксплуатации информационных и аналитических систем».

Формы, место и время проведения производственной практики

Производственная практика проходит в форме профессиональной деятельности, основанной на самостоятельном выполнении студентами производственных функций на конкретных местах, отвечающих требованиям программы практики в течение четырёх недель в 6 семестре.

Отличительной особенностью данного вида практики является ее акцент на привлечение студентов к практическому освоению программно-аппаратных средств и защищенных информационных технологий, используемых на базе практики.

Производственная практика бакалавра проводится в организациях различного характера (профиля) деятельности, форм собственности и организационно-правового статуса: в государственных и муниципальных учреждениях, в министерствах и ведомствах, департаментах различных межведомственных Комитетов, предприятиях, фирмах, корпорациях, в банках, АО, консалтинговых фирмах, научно-исследовательских институтах и центрах, вузах, а также в других структурах.

Практика может проводиться в следующих подразделениях организации:

- отделы защиты информации;
- отделы АСУ, вычислительные центры;
- отделы, занимающиеся разработкой и внедрением программного обеспечения, проектированием, монтажом и поддержкой вычислительных сетей;
- отделы, занимающиеся разработкой, продвижением и поддержкой web-сайтов.

Структура и содержание производственной практики

Общая трудоемкость производственной практики составляет 4,5 зачетных единиц, 162 часа

№	Разделы (этапы) практики	Виды производственной работы на практике, включая самостоятельную работу студентов, и трудоемкость (в часах)	Формы контроля
1	**Подготовительный**	16	Запись в дневнике практики
2	**Производственный**	100	Запись в дневнике практики
3	**Аналитический**	40	Запись в дневнике практики
4	**Отчетный**	6	Зачет с оценкой
Итого:		**162**	

Подготовительный:

Ознакомление с организацией (предприятием), правилами внутреннего трудового распорядка, производственный инструктаж, в т.ч. инструктаж по технике безопасности.

Производственный

Выполнение производственных заданий, сбор, обработка и систематизация фактического и литературного материала.

Аналитический

Анализ полученной информации, подготовка отчета по практике, получение отзыва-характеристики.

Отчетный

Сдача отчета по практике, дневника и отзыва-характеристики на кафедру, устранение замечаний руководителя практики, защита отчета по практике.

Научно-исследовательские и научно-производственные технологии, используемые на производственной практике

- Принципы моделирования объектов защиты и технических каналов утечки информации;
- Математические методы в криптологии: модели систем шифрования;
- Принципы моделей комплексных систем защиты информации (КСЗИ);
- Методы и модели оценки эффективности КСЗИ.

Учебно-методическое обеспечение самостоятельной работы студентов на производственной практике

1. Примерный перечень основных вопросов для анализа деятельности предприятия по обеспечению информационной безопасности в период прохождения производственное практики:

Общая характеристика

1. Оборот реализации продукции (услуг).

2. Общие затраты, в т.ч. на обеспечение информационной безопасности.
3. Прибыль предприятия.
4. Численность персонала.
5. Программно-техническое и коммуникационное оборудование.

Документооборот, его автоматизация и защита

1. Организационная структура предприятия и взаимосвязь подразделения информационной безопасности с другими подразделениями предприятия.
2. Документопотоки, состав технологических этапов и операций.
3. Учет конфиденциальных документов.
4. Копирование и размножение документов.
5. Формирование и хранение дел, содержащих конфиденциальные документы.
6. Учет конфиденциальных деловых (управленческих), технических, технологических и научно-технических документов в архиве.
7. Обеспечение сохранности конфиденциальных документов.
8. Оборудование архивохранилищ.

Технические средства обеспечения информационной безопасности

1. Способы и средства защиты конфиденциальной информации техническими средствами.
2. Способы устранения утечки информации по электро- радио- акустическим, оптическим и пр. каналам.
3. Организация работ по инженерно-технической защите
4. Контроль эффективности защиты информации.

Программные средства информационной безопасности

1. Методы и средства ограничения доступа к компонентам ЭВМ.
2. Защиты программ от несанкционированного копирования.
3. Пароли и ключи, организация хранения ключей.
4. Защита от разрушающих программных воздействий (РПВ) и компьютерных вирусов.

Организационные мероприятия защиты информации

1. Определение объектов защиты.
2. Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам.
3. Организация охраны предприятия.
4. Определение возможностей несанкционированного доступа к защищаемой информации.
5. Направления и методы работы с персоналом, обладающим конфиденциальной информацией.

Служба информационной безопасности на предприятии

1. Структура и штаты службы.
2. Организационные основы и принципы деятельности службы.
3. Подбор, расстановка и обучение сотрудников службы.
4. Организация труда сотрудников службы.

Формы промежуточной аттестации (по итогам производственной практики)

Промежуточная аттестация по итогам производственной практики бакалавра проводится на основании оформленного в соответствии с установленными требованиями письменного отчета, дневника практики и отзыва-характеристики руководителя практики от организации (предприятия). Дневник практики и отзыв-характеристика подписываются руководителем практики от организации (предприятия) и скрепляются печатью. Формой промежуточной аттестации является зачет с оценкой. Промежуточная аттестация проводится после выполнения программы на последней неделе практики

Учебно-методическое и информационное обеспечение производственной практики

Основная литература

1. Бабаш А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014.
2. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / - М. : РИОР : ИНФРА-М, 2013.
3. Богомолова, О. Б. Защита компьютера от вредоносных воздействий [Электронный ресурс]: практикум / - Эл. изд. - М.: БИНОМ. Лаборатория знаний, 2012.
4. Гагарина Л.Г. Разработка и эксплуатация автоматизированных информационных систем: Учебное пособие /. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013.
5. Заботина Н.Н. Проектирование информационных систем: Учебное пособие /. - М.: НИЦ Инфра-М, 2013.
6. Канцедал С.А. Алгоритмизация и программирование: Учебное пособие / - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013.
7. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие /- М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013.

Дополнительная литература

8. Аскеров Т.М. Защита информации и информационная безопасность: учебное пособие / Под общей редакцией К.И. Курбакова. - М.: Рос. экон. акад., 2001. 387с.
9. Деднев М. А., Дыльнов Д. В., Иванов М. А.: Защита информации в банковском деле и электронном бизнесе. – М.: КУДИЦ-Образ, 2004, 512 с.
10. Демушкин А.С., Куняев Н.Н., Фабричнов А.Г., Конфиденциальное делопроизводство и защищенный электронный документооборот. – М.: Логос, 2011, 452 с. ISBN: 978-5-98704-541-1
11. Партыка Т.Л., Попов И.И. Информационная безопасность: учебное пособие. − 3-е изд., перераб. и доп. М.: ФОРУМ, 2008. − 432 с.: ил.

Нормативно-правовые документы

12. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Москва. Военное издательство. 1992. 39 с.
13. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Москва. Военное издательство, 1992. 12 с.
14. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Москва, Военное издательство, 1992. 12 с.
15. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденное постановлением Правительства РФ от 3 ноября 1994 г. № 1233.

16. Требования и рекомендации по защите информации. специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Москва 2001/

17. ФЕДЕРАЛЬНЫЙ ЗАКОН “Об информации, информатизации и защите информации”. Собрание законодательства Российской Федерации. 20 февраля 1995 г. Официальное издание. Издательство “Юридическая литература”, Администрация Президента Российской Федерации. Москва с. 1213-1225.

Материально-техническое обеспечение производственной практики

ПК, стандартные офисные программные средства, программные средства борьбы со злонамеренным ПО, технические средства борьбы с утечкой информации и несанкционированным доступом к информационным ресурсам организации.

Порядок проектирования и утверждения программы производственной практики

Программа производственной практики проектируется на основе выше представленного макета с учетом требований ФГОС ВПО по соответствующему направлению подготовки и рекомендаций примерной программы. Ответственным за проектирование программы производственной практики является заведующий выпускающей кафедрой.