Минобрнауки России
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ
Проректор по учебной работе

_____ Василенко В.Н.
(подпись) (Ф.И.О.)

«26» мая 2022

ПРОГРАММА ПРАКТИКИ

УЧЕБНАЯ ПРАКТИКА
ПРАКТИКА ПО ПОЛУЧЕНИЮ ПЕРВИЧНЫХ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация (степень) выпускника

специалист по защите информации

Разработчик _____ _____ _____Скрыпников А.В._____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой _____информационной безопасности_____
(наименование кафедры, являющейся ответственной за данное направление подготовки, профиль)

_____ _____ _____Скрыпников А.В._____
(подпись) (дата) (Ф.И.О.)

1. Цели практики

Целями учебной практики является закрепление полученных теоретических знаний, знакомство с основными и вспомогательными производственными задачами; развитие практических умений и навыков исследования, анализа и описания защищенных информационных систем и связанных с ними бизнес-процессов, приобретение опыта работы в организации.

2. Задачи практики

– изучение организационной структуры предприятия и принципов управления;

– изучение и определение состава видов информационных технологий, применяемых на базе практике;

– изучение основных средств защиты информационных технологий, применяемых на базе практике (техническое, программное, лингвистическое обеспечение и т.п.);

– описание информационных ресурсов, применяемых на базе практики (базы данных, web- ресурсы, архивы и т.п.).

Объектами профессиональной деятельности специалистов являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно- технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем; системы управления информационной безопасностью автоматизированных систем.

3. Место практики в структуре образовательной программы

3.1. Учебная практика (по получению первичных профессиональных умений) относится к базовой части Блока 2 «Практики» образовательной программы.

Практика является важнейшей составной частью учебного процесса подготовки специалистов и проводится на основании учебного плана по направлению 10.05.03 – Информационная безопасность автоматизированных систем, в соответствии с требованиями Федерального Государственного образовательного стандарта высшего образования.

3.2. Для успешного прохождения практики необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: «Технологии и методы программирования», «Языки программирования», «Основы информационной безопасности», «Учебная практика (ознакомительная)».

Для освоения учебной практики студент должен:

Знать основные меры безопасности при работе с компьютером, состав, назначение функциональных компонентов и программного обеспечения персонального компьютера.

Уметь работать с офисной техникой, решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Владеть навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов).

3.3. Знания, умения и навыки, сформированные при прохождении практики, необходимы для успешного освоения последующих дисциплин «Учебная практика (по получению первичных умений и навыков научно-исследовательской деятельности»), «Безопасность персональных данных», «Безопасность сетей ЭВМ».

4. Перечень планируемых результатов обучения при прохождении практики

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

– способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

– способностью к самоорганизации и самообразованию (ОК-8);

– способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

– способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);

– способностью осуществлять поиск, изучение, обобщение и систематизацию научно- технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

– способностью создавать и исследовать модели автоматизированных систем (ПК-2);

– способностью проводить анализ защищенности автоматизированных систем (ПК-3);

– способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

– способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

– способностью разрабатывать научно-техническую документацию, готовить научно- технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

– способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

– способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);

– способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

– способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

– способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

– способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);

– способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК- 14);

– способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

– способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

– способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

– способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

– способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

– способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

– способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

– способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

– способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

– способностью обеспечить эффективное применение средств защиты информационно- технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

– способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

– способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

– способностью управлять информационной безопасностью автоматизированной системы (ПК-28).

В результате прохождения практики обучающийся должен:

Знать:

– основные принципы организации защиты информации на данной базе практики (ОК-4);

– законодательные и нормативные нормы и регламенты организации работы с персоналом (ОК-8);

– основы языков и систем программирования применительно к базе практики (ОПК-3);

– основные технологии защиты информации, используемые на предприятии (ПК-2);

– основные риски информационной безопасности (ПК-5);

– мировые и российские стандарты в области информационной безопасности (ПК-6);

– спецификации в области информационной безопасности (ПК-7);

– характеристики каналов передачи данных (ПК-10);

– компоненты системы управления информационной безопасностью автоматизированной системы (ПК-12);

– методы и средства проектирования средств защиты информации (ПК-13);

– законодательство в области сертификации средств защиты информации автоматизированных систем (ПК-15);

– нормативную документацию в области аттестации автоматизированных систем (ПК-16);

– функции межсетевых экранов. Профили защиты для межсетевых экранов (ПК-17);

– задачи систем анализа защищенности в защите открытых систем (ПК-22);

– состав информации ограниченного доступа организации (ПК-23);

– слабости системных утилит, команд и сетевых сервисов (ПК-24);

– характеристики политик информационной безопасности (ПК-27);

– функции государственной системы по обеспечению информационной безопасности (ПСК-4.1);

– понятия информационной безопасности, защиты информации, назначение и основные возможности систем защиты информации (ПСК-4.2);

Уметь:

– систематизировать и обобщать информацию (ОК-8);

– применять языки программирования в профессиональной деятельности (ОПК-3);

– применять технические и программные средства защиты информации на базе практики (ОПК-8);

– собирать информацию по обеспечению информационной безопасности предприятия (ПК-1);

– применять основные законы и нормативные документы в области информационной безопасности (ПК-3);

– проводить анализ проектных решений по обеспечению информационной безопасности (ПК-8);

– участвовать в разработке политики информационной безопасности (ПК-11);

– участвовать в контрольных проверках работоспособности применяемых программно- аппаратных средств (ПК-14);

– работать в малых коллективах в сфере обеспечения информационной безопасности (ПК-18);

– участвовать в разработке предложений по совершенствованию системы управления

– информационной безопасностью (ПК-19);

– участвовать в коллективной разработке проектов документов по обеспечению информационной безопасности (ПК-21);

– участвовать в администрировании подсистемы информационной безопасности (ПК-26);

– участвовать в работе коллектива по управлению информационной безопасностью организации (ПК-28);

– открывать и закрывать общий доступ к информации в локальной сети (ПСК-4.2);

– задавать пароли в операционной системе (ПСК-4.4);

Владеть:

– терминологией, используемой в области информационной безопасности (ОК-4);

– навыками подготовки научно-технических отчетов необходимых при организации мероприятий по защите информации (ОК-8);

– владеть информационными технологиями защиты информации на предприятии (ОПК-8);

– навыками программирования в профессиональной деятельности (ПК-4);

– способностью учувствовать в разработке защищенных автоматизированных систем (ПК-9);

– навыками эксплуатации автоматизированной системы с учетом требований информационной безопасности (ПК-20);

– навыками работы с сетевыми сканерами, сканерами безопасности (ПК-25);

– навыками программирования простейших методов шифрования-дешифрования (ПСК-4.3);

– навыками оценивания стойкости различных паролей (ПСК-4.4);

– навыками формирования ключей шифрования с заданной стойкостью (ПСК-4.5).

5. Способы и форма(ы) проведения практики

Практика является стационарной и выездной, и может проводиться в отделах защиты информации, отделах АСУ, вычислительных центрах, отделах, занимающихся разработкой и внедрением программного обеспечения, проектированием, монтажом и поддержкой вычислительных сетей, отделах, занимающихся разработкой, продвижением и поддержкой web-сайтов.

6. Структура и содержание практики

6.1. Содержание разделов практики

1) Ознакомление со структурой и работой основных подразделений предприятия, лицензией и уставом, решаемыми задачами, наличием документов разрешающих основные виды деятельности.

2) Ознакомление со структурой органов защиты информации.

3) Ознакомление с видами угроз безопасности информации, характерными для предприятия.

4) Ознакомление с видами, методами, средствами информационной защиты, применяемыми на предприятии.

6.2 Распределение часов по семестрам и видам работ по практике

Общая трудоемкость прохождения практики составляет 3 ЗЕ; 108 академических часов, 2 недели. Контактная работа обучающегося (КРо) составляет 72 ч. Иные формы работы 36 ч.

Распределение учебного времени для выполнения заданий практики:

№ п/п	Наименование разделов (этапов) практики	Часы	Формы текущего контроля
1	Ознакомление со структурой и работой основных подразделений предприятия, лицензией и уставом, решаемыми задачами, наличием документов разрешающих основные виды деятельности	10	выполнение соответствующего раздела отчета
2	Ознакомление со структурой органов защиты информации	10	выполнение соответствующего раздела отчета
3	Ознакомление с видами угроз безопасности информации, характерными для предприятия	15	выполнение соответствующего раздела отчета
4	Ознакомление с видами, методами, средствами информационной защиты, применяемыми на предприятии	12	выполнение соответствующего раздела отчета, ведение дневника практики
5	Консультации текущие с руководителем практики от университета и организации	36	выполнение соответствующего раздела отчета
6	Оформление отчета по практике	25	оформление отчета, дневника практики

7. Формы промежуточной аттестации (отчётности по итогам практики)

Отчет и дневник практик необходимо составлять во время практики по мере обработки того или иного раздела программы. По окончании практики и после проверки отчета руководителями практики от производства и кафедры, студент защищает отчет в установленный срок перед комиссией, назначаемой заведующим кафедрой.

По окончании срока практики, руководители практики от Университета доводят до сведения обучающихся график защиты отчетов по практике.

В течение двух рабочих дней после окончания срока практики обучающийся предоставляет на кафедру отчет и дневник по практике, оформленные в соответствии с требованиями, установленными программой практики с характеристикой работы обучающегося, оценками прохождения практики и качества компетенций, приобретенных им в результате прохождения практики, данной руководителем практики от организации.

В двухнедельный срок после начала занятий обучающиеся обязаны защитить его на кафедральной комиссии, график работы которой доводится до сведения студентов.

Аттестация по итогам практики проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и характеристики руководителя практики от организации. По итогам аттестации выставляется оценка (отлично, хорошо, удовлетворительно, неудовлетворительно). **Отчет и дневник** по практике обучающийся сдает руководителю практики от Университета.

8. Оценочные материалы для промежуточной аттестации обучающихся по практике

8.1. Оценочные материалы (ОМ) для практики включает в себя:

– перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

–описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

–типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

8.2. Для каждого результата обучения по практике определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

9. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

При выполнении программы практики студент может использовать учебно-методическое и информационное обеспечение дисциплин учебного плана, предшествующих выполнению программы практики.

Кроме того, необходимо использовать материалы профессиональных периодических изданий и иные информационные ресурсы.

1. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. – 5-е изд., стер. – Санкт-Петербург : Лань, 2022. – 324 с. – ISBN 978-5-8114-4067-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/206279. – Режим доступа: для авториз. пользователей.

2. Конкин, Ю. В. Основы информационной безопасности : учебное пособие / Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. – Рязань : РГРТУ, 2021. – 96 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/220418. – Режим доступа: для авториз. пользователей.

3. Горбенко, А. О. Основы информационной безопасности : ведение в профессию : учебное пособие / А. О. Горбенко. – Санкт-Петербург : Интермедия, 2016. – 336 с. – ISBN 978-5-4383-0136-3. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/90265. – Режим доступа: для авториз. пользователей.

4. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. – 2-е изд. – Москва : ИНТУИТ, 2016. – 266 с. – ISBN 978-5-94774-821-5. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/100295. – Режим доступа: для авториз. пользователей.

5. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. – 2-е изд. – Москва : ИНТУИТ, 2016. – 154 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/100296. – Режим доступа: для авториз. пользователей.

6. Загинайлов Ю. Н.Теория информационной безопасности и методология защиты информации: учебное пособие.-Директ-Медиа, 2015 https://biblioclub.ru/index.php?page=book_view_red&book_id=276557.

10. Образовательные, научно-исследовательские и научно-производственные технологии, используемые на практике

Информационно-развивающие технологии:

– использование мультимедийного оборудования при проведении практики;

– получение студентом необходимой учебной информации под руководством преподавателя или самостоятельно;

– метод IT – использование в учебном процессе системы автоматизированного проектирования.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Перечень программного обеспечения и информационных справочных систем:

1. Microsoft Office Professional Plus 2010;
2. Microsoft Office Professional Plus 2013;
3. Microsoft Office 2007;
4. Среда разработки MS Visual Studio;
5. СУБД MS SQL Server;
6. Программный пакет «Crypton LITE»;
7. Kerio WinRoute FireWall;
8. сканер безопасности «XSpider»;
9. Страж NT (версия 3.0);
10. Ревизор Сети (10 IP-адресов);
11. Ревизор-2 XP, Ревизор-1 XP;
12. Lazarus;
13. «Российское образование» - федеральный портал https://www.edu.ru/;
14. Научная электронная библиотека https://elibrary.ru/defaultx.asp;
15. Национальная исследовательская компьютерная сеть России https://niks.su/;
16. Информационная система «Единое окно доступа к образовательным ресурсам» http://window.edu.ru/;
17. Электронная библиотека ВГУИТ http://biblos.vsuet.ru/megapro/web;
18. Сайт Министерства науки и высшего образования РФ https://minobrnauki.gov.ru/;
19. Портал открытого on-line образования https://npoed.ru/;
20. Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ» https://education.vsuet.ru/.

12. Описание материально-технической базы, необходимой для проведения практики

Для проведения практики используется материально-техническая база кафедры информационной безопасности, ее аудиторный фонд, соответствующий санитарным, противопожарным нормам и требованиям техники безопасности. Кафедра располагает наличием компьютерных классов (аудиториями (а. 332а, 420, 424), оснащенными в каждой аудитории 12 ПК Intel Core 2 Duo персональных компьютеров) с выходом в сеть «Интернет» и установленным лицензионным программным обеспечением (Microsoft Windows 8.1, Microsoft Office 2013, AutoCAD, САПР КОМПАС и др.).

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем.