

Парламентское собрание Союза Беларуси и России
Постоянный Комитет Союзного государства
Оперативно-аналитический центр
при Президенте Республики Беларусь
Государственное предприятие «НИИ ТЗИ»
Полоцкий государственный университет



КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Бен+2)
К63

К63

Комплексная защита информации : материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных направлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Бен+2)

ЧТО ДОЛЖЕН УМЕТЬ НАЧИНАЮЩИЙ СПЕЦИАЛИСТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ВЗГЛЯД КОМПАНИИ-РАЗРАБОТЧИКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

С.П. ПАНАСЕНКО

ООО Фирма «АНКАД»

По оценкам, прозвучавшим в кулуарах V Форума Ассоциации защиты информации в 2016 г., около 70 % выпускников специальностей, связанных с информационной безопасностью (ИБ), после окончания института уходят работать в качестве специалистов в организации, эксплуатирующие средства защиты информации (СЗИ).

Ясно, что значительно меньший процент таких выпускников достается компаниям, занимающимся разработкой средств защиты. Тем не менее, выпускники, получающие в высших учебных заведениях знания по информационной безопасности, востребованы и в организациях-разработчиках СЗИ. Поэтому хотелось бы в данном докладе предложить взгляд ООО Фирма «АНКАД» – достаточно известного в России разработчика СЗИ – на требования к подготовке специалистов в области ИБ.

Отметим, что по данному вопросу взгляды компаний-разработчиков СЗИ во многом совпадают, поэтому приведенные далее требования можно рассматривать как общее мнение Фирмы «АНКАД» и ряда ее партнеров, также являющихся разработчиками СЗИ.

Студент или выпускник может трудоустроиться в компанию, разрабатывающую СЗИ, как минимум, на следующие направления работы:

- в качестве разработчика программного или аппаратного обеспечения;
- в качестве инженера по тестированию, по технической поддержке, по системной интеграции и т. п.;
- в качестве инженера-исследователя;
- в качестве менеджера по маркетингу.

В зависимости от конкретного направления работы требования к начинающим специалистам могут значительно различаться. Сформулируем основные требования, предъявляемые к выпускникам в зависимости от направления (для некоторых из перечисленных выше направлений):

1. Требования к программистам:

- знание базовых алгоритмов и структур данных;
- понимание, как минимум, основных принципов работы операционных систем: виртуальная память, адресация, пэйджинг; режим ядра и пользовательский режим; процессы и потоки, многозадачность, синхронизация; сети и сетевые протоколы...;
- понимание концепций безопасного программирования и обработки ошибок, принципов организации кода;
- понимание работы средств сборки программного обеспечения: компиляторов, компоновщиков, интерпретаторов;
- могут потребоваться знание и опыт применения конкретных языков программирования, средств разработки, надстроек и т. п., а также знание требований стандартов единой системы программной и/или конструкторской документации (ЕСПД/ЕСКД).

2. Требования к инженерам по тестированию, технической поддержке, системной интеграции:

- знание компьютерного оборудования, опыт подбора требуемых комплектующих и сборки компьютеров;

знание основных операционных систем, опыт установки и настройки операционных систем и программного обеспечения (т. е., как минимум, офисных и графических пакетов, средств разработки, средств коммуникации и т. п.);

знание и понимание принципов работы компьютерных сетей, умение прокладки сетей, установки и настройки сетевого оборудования;

творческий подход к поиску ошибок и их устранению;

для инженеров по тестированию также требуется понимание основных принципов тестирования, включая методы его автоматизации.

3. Требования к инженерам-исследователям:

грамотность, что подразумевает уверенное владение письменным русским языком;

уверенная работа с компьютером в качестве, как минимум, продвинутого пользователя, уверенно использующего основные операционные системы и приложения, включая офисные;

опыт исследовательской работы;

наличие публикаций и/или выступлений на конференциях различного уровня;

нацеленность на достижение в перспективе заметных научных результатов и получение ученой степени.

4. Требования к менеджерам по маркетингу (в обязанности которых обычно входят, помимо прочего, вопросы предпродажной подготовки и сопровождения продаж):

понимание порядка регулирования рынка защиты информации: регуляторы, законодательство; лицензирование, сертификация, аттестация и т. д.;

понимание основ работы компьютера, сервера, телекоммуникационных сетей;

понимание принципов построения защиты объектов информатизации;

умение работать с компьютерным оборудованием – как минимум, для проведения демонстраций клиентам продукции компании, включая настройку оборудования и соответствующего программного обеспечения;

грамотная устная и письменная речь, навыки написания текстов, умение структурированно излагать мысли.

При этом для трудоустройства в компанию, разрабатывающую СЗИ, однозначным плюсом для соискателя будет наличие хорошо структурированных знаний в области ИБ, включая как знания в части технической защиты информации, так и знания криптографических методов и средств защиты, а также требований к средствам защиты со стороны регуляторов. Это касается всех описанных выше направлений.

Таким образом, в компанию-разработчик СЗИ на различные позиции первоочередно рассматриваются кандидаты, закончившие высшие учебные заведения именно как специалисты по ИБ.

Однако, с другой стороны, подавляющее большинство рассмотренных нами кандидатов, закончивших институты по направлениям, связанным с ИБ, не обладает достаточными знаниями и опытом в части других предъявляемых требований. Особенно это касается недостаточного (в большинстве случаев) уровня знаний компьютерного и сетевого оборудования, что мы считаем обязательным требованием для практически любого специалиста, планирующего работать в компании-разработчике СЗИ.

Поэтому мы призываем руководителей профильных кафедр высших учебных заведений, выпускающих специалистов в области ИБ, уделять в образовательном процессе особое внимание курсам, связанным с вопросами разработки и функционирования компьютерного оборудования и программного обеспечения, а также с вопросами построения компьютерных сетей, работы сетевого оборудования и используемых сетевых

протоколов для различных способов передачи данных. Теоретические и практические знания по данным вопросам, на наш взгляд, однозначно пригодятся ИБ-специалистам в их последующей работе.

В текущем году Фирма «АНКАД» выпускает сборник лабораторных работ под названием «Практические методы обеспечения безопасности информационных ресурсов с использованием средств защиты информации серии «КРИПТОН». Он посвящен, в основном, средствам защиты информации от несанкционированного доступа и ряду смежных направлений. Сборник включает в себя следующие лабораторные работы:

1. Обеспечение санкционированного доступа на сервер корпоративной сети с использованием программного комплекса «Crypton Lock 3.5».
2. Разграничение и контроль доступа пользователей к техническим средствам вычислительной сети с использованием аппаратно-программного модуля доверенной загрузки «КРИПТОН-ЗАМОК».
3. Двухфакторная аутентификация в службе каталогов Active Directory с использованием USB-идентификатора «РУТОКЕН».
4. Исследование средств защиты информации, хранящейся на жёстких дисках, на примере комплекса «Crypton Disk».
5. Исследование средств защиты информации с использованием электронной цифровой подписи.
6. Исследование криптографических средств защиты информации при сетевом взаимодействии на примере программного комплекса «Crypton IPMobile».
7. Исследование возможностей по управлению USB-идентификатором «РУТОКЕН» с помощью APDU-команд.

Во всех этих лабораторных работах, помимо изучения на практике основных вопросов, вынесенных в заглавия работ, от студентов требуется изучение и последующее выполнение ряда действий по настройке компьютерного оборудования и программного обеспечения, поскольку это требуется для функционирования изучаемых СЗИ. Такая настройка включает в себя:

- установку и настройку программного обеспечения, в т. ч. драйверов устройств;
- работу в гостевых виртуальных машинах и их настройку, включая «проброс» функций аппаратного обеспечения в гостевые операционные системы;
- настройку локальных сетей и др.

Подобные лабораторные работы позволят ИБ-специалистам получить некоторые из перечисленных выше требуемых знаний. На наш взгляд, специалисты по информационной безопасности обязательно должны обладать знаниями того аппаратного и программного окружения, в котором будут работать разрабатываемые или эксплуатируемые ими средства защиты, а также опытом работы с применяемым аппаратным и программным обеспечением.

ЗАЩИТА ИНФОРМАЦИИ В УГОЛОВНОМ ПРОЦЕССЕ

Т.В. РАДЫНО

ООО «Минский электротехнический завод имени В.И. Козлова»

Задачами уголовно-процессуального закона являются закрепление надлежащей правовой процедуры осуществления уголовного процесса, обеспечение законных прав и интересов физических и юридических лиц, которым преступлением причинен физи-