НАПРАВЛЕНИЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРУГРОЗАМ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ

Шеремет И.А.[1]

В статье рассмотрены новые угрозы автоматизированным системам банковско–финансового сектора со стороны киберпреступности и направления работы Финансового университета при Правительстве Российской Федерации по подготовке специалистов по информационной безопасности для кредитно–финансовых организаций. Требуемые специалисты должны обладать широким спектром компетенций, и именно в Финуниверситете, как ни в каком другом ВУЗе страны, могут быть учтены все особенности, связанные с преподаванием групп дисциплин финансовой, экономической, правовой и информационно–технологической направленности. Специалисты данного профиля, обладающие всеми необходимыми знаниями, навыками и умениями, в полной мере охватывающими инженерно–технические и организационно–правовые аспекты кибербезопасности, смогут найти достойное применение в кредитно–финансовых организациях.

***Ключевые слова**: киберпреступность, информационная безопасность, кибербезопасность, практико–ориентированное обучение.*

DOI:10.21681/2311-3456-2016-5-3-7

Введение

Переживаемый человечеством период времени характеризуется постоянным ростом влияния информационных технологий на человека и его деятельность. Наблюдается интенсивное воздействие информационной сферы на психику и поведение отдельных лиц и целых социальных групп. Инфосфера сегодня активно влияет на состояние политической, финансово-экономической, оборонной и других базисных составляющих безопасности любого государства. Общепринятым фактом считается то, что национальная безопасность сегодня существенным образом зависит от комплексного обеспечения информационной и экономической безопасности, и по мере развития глобальной информационной инфраструктуры эта зависимость только возрастает [1].

В течение последних двух десятилетий ведущие страны мира активно отрабатывают тактику и стратегию ведения информационных войн [1,2,3]. Различные аспекты и приемы информационной экспансии, наблюдаемые повсеместно, подпитывают новыми идеями и возможностями киберпреступность и, прежде всего, в ее проявлениях в кредитно-финансовой сфере (КФС), где количество попыток проведения кибератак растет практически ежемесячно. Причем под угрозой похищения денежных средств или дезорганизации работы с целью их вымогательства оказываются не только банки и их клиенты, но и другие критически важные объекты информационной инфраструктуры, участвующие в денежном обороте. Современные киберпреступники действуют все более скрытно и наносят все более серьезный ущерб, используя при этом похищенные персональные данные, методы социальной инженерии и фишинга, проводя вирусные атаки и атаки на веб-сайты с целью похищения данных для их последующей перепродажи. Киберпреступникам удалось извлечь из, казалось бы, абсолютно защищенных баз данных американского Чейз Манхэттен Банка сведения о счетах более 8 миллионов бизнес-структур и 74 миллионов физических лиц [3]. Только в 2015 г. в России ущерб от 43 тыс. киберпреступлений составил порядка 400 млрд. руб. против 217 млрд. руб. от 74 тыс. преступлений экономического характера [4]. По данным одного из ведущих производителей средств обеспечения кибербезопасности компании Symantec, в 2015 году в мире киберпреступностью похищено более 158 млрд. долларов США.

Новые вызовы – новые требования

По мнению специалистов Symantec, опубликовавших свои прогнозы в области обеспечения безопасности и хранения данных, в 2017 году на передний план выйдут «облака», виртуализация, а также безопасность мобильных устройств и социальных сетей.

1 ШереметИгорь Анатольевич, член-корреспондент РАН, доктор технических наук, профессор, заведующий кафедрой «Информационная безопасность» Финансового Университета при Правительстве Российской Федерации, г. Москва, IASheremet@fa.ru

Миллиарды людей пользуются мобильными телефонами с возможностью выхода в Интернет. Ранее киберпреступники не проявляли большого интереса к мобильным устройствам, но по мере повышения интеллектуального уровня этих устройств и формирования платформ-лидеров в данном сегменте рынка преступники неизбежно будут направлять свои атаки на мобильные устройства. Следовательно, будет расти объем конфиденциальных данных, утерянных через эти устройства.

Схожие проблемы создает и широкое распространение виртуализации. Быстрое и разобщенное внедрение виртуальных инфраструктур, а также отсутствие стандартов на их построение и функционирование будут продолжать создавать бреши в безопасности при резервном копировании и обеспечении высокой готовности виртуальных сред. И хотя виртуализация снижает затраты на серверную инфраструктуру, отечественные и зарубежные кредитно-финансовые организации (КФО) приходят к пониманию того, что она одновременно создает новые угрозы безопасности данных. Еще более усложняет ситуацию с кибербезопасностью использование социальных сетевых сервисов для повышения уровня коммуникаций и персональной эффективности сотрудников КФО.

Для адекватного реагирования на новые вызовы и соответствия новым требованиям к сотрудникам подразделений информационной безопасности требуется использовать компетентностный подход в подготовке специалистов в области кибербезопасности, означающий ориентацию образовательных программ на практическую подготовку, на выработку у студентов умения решать реальные задачи в соответствующих областях деятельности.

Новые компетенции

Необходимость поиска и применения адекватных мер противодействия кибермошенничеству, защиты банковских продуктов и информационной инфраструктуры кредитно-финансовой сферы обуславливают пристальное внимание общества к качеству подготовки специалистов по противодействию киберугрозам КФО.

Какими же компетенциями в области кибербезопасности должны обладать выпускники ВУЗов? Как представляется, эти компетенции должны охватывать следующие основные направления.

Фундаментальные знания в области информационных технологий и кибербезопасности:

- архитектура и организация функционирования ЭВМ;
- современные вычислительные системы и сети связи, сетевые технологии;
- администрирование современных операционных систем;
- администрирование баз данных;
- работа с большими данными;
- системы искусственного интеллекта;
- средства мониторинга информационных сетей;
- уязвимости современных программных и аппаратно-программных средств ; общие методы и средства обеспечения информационной безопасности; защищенные сетевые технологии глобального, корпоративного и локального назначения;
- математические аспекты защиты информации, криптографии, стеганографии, криптоанализа;
- способы и средства разработки защищенных приложений;
- системотехника и схемотехническое проектирование аппаратных средств информационной безопасности;
- построение и функционирование электронных платежных систем.

Понимание технологий реализации угроз информационной безопасности:

- программирование в современных операционных средах;
- анализ алгоритмов;
- реверс-инжиниринг программных текстов;
- атаки на электронные платежные системы;
- поиск следов и методы расследования киберпреступлений в кредитно-финансовой сфере.

Понимание принципов управления бизнесом и обеспечения его информационной безопасности:

- гражданско-правовые отношения;
- основы управления предприятием и организацией;
- описание бизнес-процессов;
- основные бизнес-процессы банка;
- нормативная база Центрального банка Российской Федерации;
- нормативно-правовая база информационной безопасности;
- автоматизированные системы обработки, хранения и передачи информации с учетом уровней и критериев безопасности.

Лидерские качества и презентационные навыки:

- основы социологии;
- основы психологии;
- технологии разработки бизнес-планов, методы командной работы;

– тайм-менеджмент;
– личная эффективность;
– планирование деятельности;
– дизайн-мышление;
– инструменты создания презентаций.

Понимание принципов управления рисками:

– международные стандарты управления рисками и информационной безопасности;
– Базельские стандарты;
– теория вероятностей и математическая статистика;
– теория игр;
– оценка экономической эффективности.

Три направления работы финуниверситета в области подготовки специалистов по информационной безопасности для кредитно-финансовой сферы

В целях всестороннего обеспечения учебного процесса, направленного на подготовку специалистов, обладающих приведенными выше компетенциями, в Финуниверситете предусматривается развертывание деятельности по трем ключевым направлениям:

– организация взаимодействия с кредитно-финансовыми организациями – работодателями для выпускников ВУЗа;
– совершенствование образовательного процесса и уровня подготовки профессорско-преподавательского состава;
– повышение уровня подготовки студентов.

В рамках *первого* из перечисленных направлений при кафедре «Информационная безопасность» в январе 2016 года создана межведомственная рабочая группа (МРГ), включающая ответственных сотрудников подразделений кибербезопасности Банка России, Ассоциации российских банков, Национальной системы платежных карт, Ассоциации «Финансовые инновации», Сбербанка, МВД России, Росфинмониторинга, Роснаркоконтроля, а также Минобороны России, которая предназначена для формирования и, при необходимости, оперативной корректировки учебных программ по специальностям кафедры. К настоящему времени все материалы, подготовленные кафедрой для организации учебного процесса в 2016-2017 учебном году, согласованы МРГ.

Наряду с этим предусматривается реализация следующих основных принципов взаимодействия Финуниверситета с кредитно-финансовыми организациями:

– закрепление за КФО роли стратегических партнеров в области подготовки специалистов по информационной безопасности для этих организаций;
– проактивное формирование кредитно-финансовыми организациями кадрового резерва служб кибербезопасности из студентов Финуниверсистеита, обучающихся на кафедре «Информационная безопасность»;
– доступ кафедры к компетенциям специалистов КФО и их информационно-технологической базе при планировании и реализации учебного процесса;
– организация выполнения кафедрой научно-исследовательских работ в интересах КФО;
– спонсорская и благотворительная поддержка кафедры со стороны КФО.

Второе направление предполагает реализацию следующих мероприятий:

– постоянное обучение преподавателей в различных центрах повышения квалификации по специальности «Информационная безопасность» и смежным специальностям;
– получение профессорско-преподавательским составом грантов на выполнение исследований в рамках конкурсов, проводимых Российским фондом фундаментальных исследований, Российским научном фондом и другими грантообеспечивающими организациями;
– разработка целевых программ для реализации непрерывного образования.

Третье направление предполагает реализацию следующих видов деятельности:

– организация практико-ориентированного обучения студентов, включая учебные курсы и кейсы от сотрудников кредитно-финансовых организаций;
– мастер-классы, проводимые ведущими специалистами КФО;
– студенческие олимпиады по кибербезопасности;
– хакатоны (от англ. Hackathon = Hackers Marathon), посвященные различным направлениям реализации возможных угроз информационной безопасности объектов кредитно-финансовой сферы;
– практика и стажировка студентов в КФО;
– проектная деятельность студентов в соответствующих подразделениях КФО.

Возможности финуниверситета по подготовке специалистов по информационной безопасности для кредитно-финансовых организаций

Исходя из изложенного, кафедрой «Информационная безопасность» Финансового универси-

тета при Правительстве Российской Федерации совместно с представителями подразделений информационной безопасности ряда кредитно-финансовых организаций были разработаны требования к уровню подготовки выпускников по данному направлению и соответствующие учебные программы.

Внедрение в Финуниверситете нового профиля подготовки «Информационная безопасность автоматизированных банковских систем» обусловлено тем, что именно здесь в последние годы были достигнуты определенные положительные результаты и накоплен уникальный опыт по подготовке специалистов, получающих знания в области безопасности информации финансово-экономического характера и одновременно навыки и умения по применению методов и технических средств защиты информации. При этом потребность в базовых знаниях, касающихся всего информационно-технологического контура сбора, обработки и использования информации, значительных объемов данных как о защищаемых объектах, так и о возможностях киберпреступности потребовала объединения усилий различных кафедр в рамках единого образовательного процесса.

В основу системы подготовки кадров в области информационной безопасности в Финуниверситете положен принцип сочетания «вертикали» - с охватом всех уровней подготовки, - и «горизонтали» - с выходом на проблемы информационной безопасности в гуманитарной сфере и на стыке естественно-научных, технических и гуманитарных направлений.

В настоящее время преподавание дисциплин в области информационной безопасности в кредитно-финансовой сфере в Финуниверситете ведется профильной кафедрой «Информационная безопасности» во взаимодействии с кафедрой «Анализ рисков и экономическая безопасность». Необходимо отметить, что на базе именно этих кафедр планируется проводить основной учебный процесс по обучению студентов (бакалавриат, магистратура, аспирантура), а также по повышению квалификации и профессиональной переподготовке специалистов в области информационной безопасности для КФО, а также по иным направлениям в области информационной безопасности для соответствующих предприятий правоохранительной, оборонной и научной сфер.

На наш взгляд, наряду с техническими знаниями будущим специалистам необходима также основательная правовая подготовка и детальная проработка экономических аспектов обеспечения информационной безопасности в условиях активного информационного противоборства. В первую очередь это относится к подготовке и переподготовке специалистов для правоохранительных органов, а также органов суда и прокуратуры в области борьбы с преступлениями в сфере кибербезопасности.

Специалисты нового уровня должны не только уметь адаптировать общие требования нормативно-правовых актов в области информационной безопасности к условиям функционирования конкретной организации, но и участвовать в разработке и практической реализации проектов по созданию современных интегрированных интеллектуальных систем безопасности в КФО. В процессе обучения специалисты должны не только овладеть навыками практической работы на самом современном оборудовании, но и принимать активное участие в НИР и ОКР по разработке перспективных методов и средств комплексной защиты информации для КФО. Естественно, подготовка таких высококвалифицированных кадров должна опираться на соответствующую материально-техническую базу. А такое под силу только крупному ВУЗу – исследовательскому центру, которым и является Финуниверситет.

Одним из важных условий повышения качества подготовки специалистов в области информационной безопасности является формирование высоких нравственных качеств у студентов. И здесь «человеческий фактор» - это интегральная характеристика личности, определяющая надежность защиты информации при ее получении, хранении и переработке в автоматизированных банковских системах. Невзирая на разнообразие и постоянное совершенствование специальной техники для защиты информации, люди остаются самым слабым звеном в человеко-машинных системах, одним из самых вероятных источников утечки информации, в связи с чем наибольшим ущербом чреваты атаки на информационные и аппаратно-программные ресурсы кредитно-финансовых организаций с использованием инсайдеров. Поэтому проблему «человеческого фактора» при подготовке специалистов в области информационной безопасности целесообразно решать в двух направлениях: совершенствование технологии профессионального отбора на специальности, связанные с защитой информации, и оптимизация воспитательной работы в процессе обучения.

Заключение

Финансовым университетом при Правительстве Российской Федерации развернута работа по подготовке специалистов нового уровня, способных обеспечить информационную безопасность кредитно-финансовых организаций России в условиях роста числа и сложности угроз, реализуемых международной киберпреступностью. В этой работе Финуниверситет опирается на взаимодействие с подразделениями кибербезопасности ключевых объектов кредитно-финансовой сферы нашей страны. Конечной целью прилагаемых в данном направлении усилий является создание такой системы подготовки специалистов, которая обеспечивала бы пополнение указанных подразделений высококвалифицированными кадрами, способными качественно решать возложенные на них сложнейшие задачи немедленно по прибытии на свои рабочие места по окончании ВУЗа. Финуниверситет обладает практически всеми ресурсами, необходимыми для подготовки таких специалистов.

***Рецензент**: Лебедь Сергей Васильевич, канд. техн. наук, управляющий директор – заместитель начальника департамента безопасности ПАО «Сбербанк», SVLebed@sberbank.ru.*

Литература

1. Шеремет И. А. Киберугрозы России растут. – Военно-промышленный курьер, 2014, №№ 5-6.
2. Жуков И. Ю., Михайлов Д. М., Шеремет И. А. Защита автоматизированных систем от информационно-технологических воздействий. – М.: МИФИ, 2014.
3. Троянский код. Интервью с членом коллегии Военно-промышленной комиссии Российской Федерации И.А. Шереметом. – Российская газета, 21 ноября 2014 г.
4. Материалы встречи заместителя председателя правления ПАО «Сбербанк» С.К. Кузнецова с представителями ВУЗов 15 июля 2016 года. - М.: 2016.

DIRECTIONS OF A NEW LEVEL EDUCATION TO COUNTER CYBERTHREATS IN FINANCIAL SPHERE

***Sheremet I.A.*[2]**

The article describes new challenges of cybercrime in the financial sphere and new approaches to distinguished cybersecurity specialists high quality education and training implemented by Financial University under the Government of Russian Federation. These specialists would have comprehensive knowledge in financial, economical, legal and information technology areas. Possessing all the necessary knowledge and skills, fully covering all technological and legal aspects of the cybersecurity, they would be able to solve all the complicated problems they will face while serving in banks and financial structures.

***Keywords**: cybercrime, information security, cybersecurity, practice–oriented education and training.*

References

1. Sheremet I.A. Cyberthreats to Russia are growing. – Military - industrial courier, 2014, No. 5 - 6.
2. Zhukov I.Yu., Mikhailov D.M., Sheremet I.A. Computerized systems defence from the infotechnological impacts. – Moscow: MEPhI, 2014.
3. The trojan code. Interview with member of the Board of Military - industrial commission of Russian Federation Igor Sheremet. – Rossiyskaya gazeta, November 21, 2014.
4. Content of the meeting of the deputy chairman of the Board of PJSC «Sberbank» S. K. Kuznetsov with representatives of Universities on 15 July 2016. – Moscow: 2016.

2 Igor Sheremet, Corresponding member of RAS, Doctor of Sciences (in Tech.), Professor, head of the Information security department of the Financial University under the Government of Russian Federation, Moscow, IASheremet@fa.ru