Проверка на прочность с признаками эффективности

Истоки создания учебной базы для подготовки специалистов связи в нашей республике восходят к началу 30-х годов прошлого века. Это заслуживает отдельного и подробного повествования. Но истории, как известно, свойственен поступательный характер, который особенно рельефно проявился в процессе преобразования Высшего государственного колледжа связи в учреждение образования «Белорусская государственная академия связи». Это было в октябре 2015 года. Каковы результаты данной реконструкции?

ЗЕНЕВИЧ А.О.,
ректор,

КУДРИЦКАЯ Е.А.,
проректор по учебной работе,

ДОМАКУР О.В.,
ученый секретарь,

Белорусская государственная академия связи

В 2015 году Высший государственный колледж связи был преобразован в учреждение образования «Белорусская государственная академия связи». Перед руководством реформированного вуза стояла задача вывести высшее специальное образование на новый уровень, отвечающий актуальным вызовам времени.

Гарантированным подтверждением качества обучения в Академии связи за эти годы стала напряженная работа, масштабы которой привели учебное заведение к высоким результатам. Ежегодно выполняются контрольные цифры набора и приема абитуриентов, а все выпускники распределяются на первые рабочие места.

За 5 лет успешно пройдены пять государственных аккредитаций:

- на соответствие заявленному виду «колледж» и по специальностям;
- на соответствие заявленному виду «академия» и по специальностям;
- по специальностям высшего образования I и II ступени;
- по укрупненным специальностям магистратуры;
- на соответствие заявленному виду и по специальностям и государственная аккредитация по специальностям высшего образования I и II ступени.

Ежегодно Академия связи проводит сертификацию системы менеджмента качества на соответствие требованиям стандарта ISO СТБ 9001-2015.

За минувший период открыты:

- 5 специальностей магистратуры: 1-26 80 09 «Государственное управление»; 1-31 80 07 «Радиофизика»; 1-53 80 01 «Автоматизация»; 1-26 81 12 «Электронное правительство»; 1-53 80 01 «Автоматизация и управление технологическими процессами и производствами (по отраслям)»; 1-98 80 03 «Аппаратное и программно-техническое обеспечение информационной безопасности»;
- 2 специальности аспирантуры: 05.11.13 «Приборы и методы контроля природной среды, веществ, материалов и изделий», 05.12.13 «Системы, сети и устройства телекоммуникаций (технические науки)»;
- 2 специальности переподготовки руководящих работников и специалистов, имеющих высшее образование 1-40 01 73 «Программное обеспечение

информационных систем», руководящих работников и специалистов, имеющих среднее специальное образование 2-40 01 71 «Тестирование программного обеспечения».

По предложению академии связи новый профиль среднего специального образования «Информационные кабельные сети» введен в Общегосударственный классификатор Республики Беларусь ОКРБ 011-2009 «Специальности и квалификации» (Изменение № 30), разработаны типовой учебный план и образовательный стандарт по данной специальности. В планах вуза с сентября 2021 года начать обучение по данной специальности.

В период пандемии COVID-19 с апреля 2020 года начала функционировать Платформа удаленного обучения. На ее основе организовано проведение занятий в период сложной эпидемиологической ситуации. В Государственном регистре электронных информационных ресурсов разработаны и зарегистрированы 260 электронных учебно-методических комплексов по дисциплинам. Издано 27 учебников и учебных пособий с грифом Министерства образования Республики Беларусь.

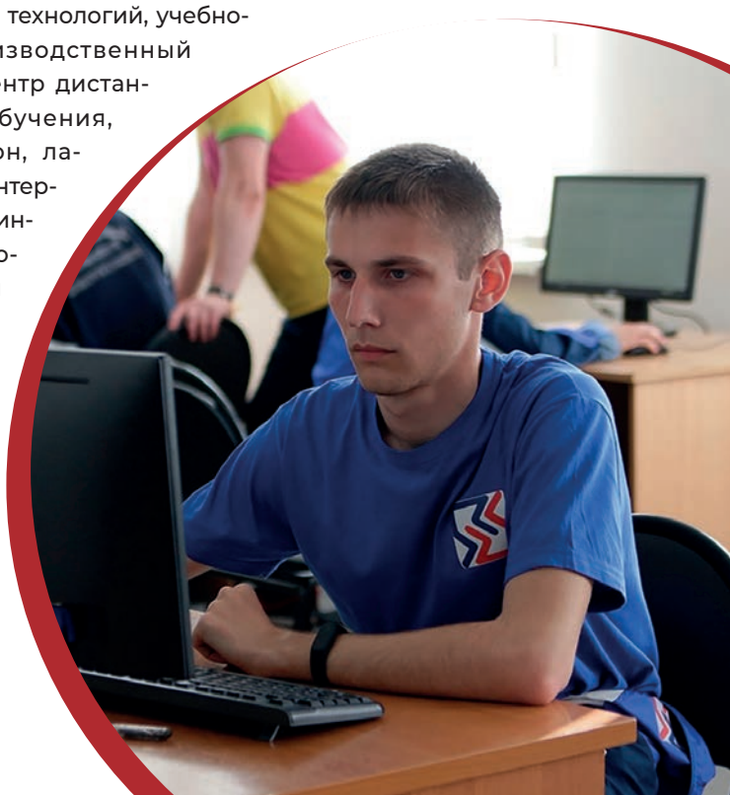
Организовано обучение на английском языке иностранных граждан по специальностям: 1-45 01 02 02 «Инфокоммуникационные системы», 2-40 01 31 «Тестирование программного обеспечения».

Творческие и научные усилия академии связи в течение пяти минувших лет достойно отмечены со стороны государства. Например, 72 выпускника вуза получили дипломы с отличием, стипендии специального фонда Президента Республики Беларусь за высокие достижения в учебе назначены 26 студентам,

13 студентов награждены премией специального фонда Президента Республики Беларусь за победы в республиканских и международных конкурсах профессионального мастерства.

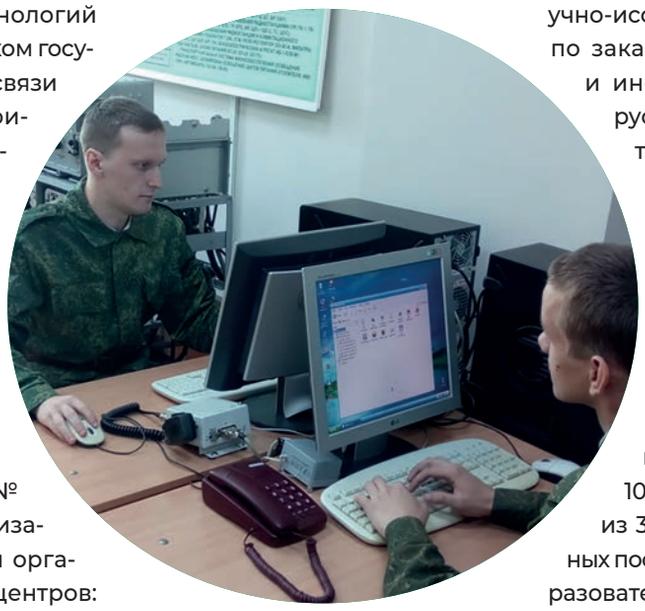
В академии связи созданы новые структуры: обособленное подразделение «Колледж информационно-коммуникационных технологий», факультет довузовской подготовки, кафедра довузовского образования и русского языка как иностранного, военная кафедра, научно-технический отдел, отдел аспирантуры и международной деятельности, группа по защите государственных секретов, отраслевая лаборатория современных инфомационно-коммуникационных технологий, учебно-научно-производственный комплекс, центр дистанционного обучения, киберполигон, лаборатория «интернета вещей», информационно-обучающий центр IP-телефонии.

За минувшие пять лет учебный процесс в вузе максимально



приближен к практике. На производстве созданы 6 филиалов кафедр: филиал кафедры телекоммуникационных систем в ОАО «Гипросвязь», филиал кафедры организации и технологий почтовой связи в Брестском государственном колледже связи и на РУП «Белпочта», филиал кафедры инфокоммуникационных технологий в ООО «Ай Ди Эй Технолоджис», филиал кафедры радио и информационных технологий в НИУП «Институт цифрового телевидения Горизонт», филиал кафедры цифровой экономики в гимназии № 28 г. Минска. Для организации обучения учащихся организованы 5 ресурсных центров: LingvaLand, «Обучение лиц с нарушениями слуха современным инфокоммуникационным технологиям», «Технологии почтовой связи», «Направляющие системы телекоммуникаций», «Мультимедийные информационные технологии».

Сегодня академия связи располагает основательной научной базой, на основе которой функционируют 4 научно-педагогические школы: «Квантовые информационные системы», «Инфокоммуникационные системы и устройства», «Информационное управление в телекоммуникационных системах», «Теория экономического роста страны и ее инновационная и структурная составляющие». В вузе образованы 7 международных научных лабораторий совместно с университетами Украины, Азербайджана, Узбекистана, Кыргызстана.



На счету академии связи – 9 патентов, выполнены 22 научно-исследовательские работы по заказу Министерства связи и информатизации и Белорусского фонда фундаментальных исследований, реализовано 20 инициативных научно-исследовательских работ. Объем финансирования научной деятельности ежегодно увеличивался.

В течение 5 лет в вузе прошли обучение около 1000 иностранных граждан из 30 стран. Сумма экспортных поступлений от оказания образовательных услуг увеличивалась ежегодно в среднем на 62 %.

Сегодня, помимо прочего, очевидно, что одним из достоинств учреждения образования «Белорусская государственная академия связи» является способность оперативно реагировать на потребности рынка труда. Вуз выбрал свою образовательную траекторию развития.

Повергнуть нельзя смириться

Пандемия коронавирусной инфекции COVID-19 беспрецедентно повлияла на различные области человеческой жизнедеятельности. Не остался в стороне и ее современный технологический уклад. Например, массовая удаленная работа не могла не сказаться на состоянии кибербезопасности как бизнеса и госучреждений, так и обычных пользователей.

Эксперты известной российской компании Positive Technologies, партнеры нашего журнала, рассказали о тенденциях кибербезопасности, которые сложились в 2020 году, а также поделились своими прогнозами на будущее.

– Из-за повсеместного внедрения удаленной работы в минувшем году появились новые риски информационной безопасности, – говорит Алексей Новиков, директор экспертного центра безопасности Positive Technologies. – Глобальный новостной повод – эпидемию – использовали все типы хакерских группировок. Нашими сотрудниками за минувший год было проведено 47 расследований. В числе ключевых тенденций эксперты Positive Technologies отметили целый ряд наиболее острых с далеко идущими последствиями.

Какова же обратная сторона удаленки?

По мнению экспертов, переход на удаленный режим работы спровоцировал во всем мире рост числа атак, направленных на эксплуатацию уязвимостей в корпоративных сервисах, доступных из интернета. Ведь компании в срочном порядке выводили сервисы на периметр. Выросло число узлов, в частности, российских компаний с доступным для подключения RDP. Как следствие, доля атак с эксплуатацией уязвимостей в ПО и недостатков конфигурации ближе к концу 2020 года увеличилась до 30 % (в I квартале было 9 %).

Еще один тренд, появившийся на фоне пандемии, – атаки, направленные на кражу учетных данных для подключения к системам аудио- и видеосвязи Skype, Webex и Zoom, а также вмешательство в конференции.

Актуальным в минувший период явился бум шифровальщиков.

В течение минувшего года наблюдалось постоянное увеличение числа атак шифровальщиков. Если в первом квартале для организаций доля шифровальщиков

в атаках с использованием ВПО составляла 34 %, то в третьем квартале она достигла 51 %. Операторы шифровальщиков все реже проводят массовые атаки, они целенаправленно выбирают крупные компании, которые в состоянии заплатить большой выкуп, или организации, для которых приостановка деятельности опасна, и наносят точечные удары.

Особую проблему, по мнению экспертов Positive Technologies, представляли атаки на цепочку поставок. Настоящей болью в 2020 году стали supply chain attacks.

– В нашей практике мы сталкивались с такими же атаками на разработчиков ПО и средств защиты, на IT-интеграторов, подрядчиков IT-компаний, на порталы государственных организаций в различных странах, – продолжает Алексей Новиков. – Уровень защищенности крупных компаний повышается, и их становится все сложнее взламывать, особенно если целью злоумышленников является долговременное присутствие, а не разовая атака. И поэтому APT-группировки все чаще стали атаковать партнеров и поставщиков жертвы. Защититься от подобных атак очень сложно, это под силу только высококлассным специалистам в области ИБ.

На повестке информационной безопасности минувшего года возникло такое явление, как выкуп за неразглашение. Шантаж публикацией данных в случае отказа жертвы платить выкуп был поставлен на поток. Наибольшую активность в таких атаках в 2020 году проявили операторы Maze, Sodinokibi, DoppelPaymer, NetWalker, Ako, Nefilim, Clop. Многие операторы шифровальщиков сделали собственные сайты и даже организуют аукционы по продаже украденных данных.

Своеобразным преступным промыслом в ушедшем году был доступ на продажу, когда киберпреступники покупали доступы в организации-жертвы у других злоумышленников. Одними из первых по такой схеме стали действовать операторы шифровальщиков: они предлагали сотрудничество, искали партнеров для распространения их трояна-вымогателя и обещали своим подельникам долю от суммы выкупа. Рынок доступов к сетям компаний в дарквебе позволял воровать низкоквалифицированным хакерам, которые могут ограничиться поиском уязвимостей на внешних ресурсах компаний с целью продажи.

Как на ладони оказались проблемы промышленного и энергетического секторов. В 2020 году было зафиксировано около 200 атак на предприятия из этих отраслей, что почти на 60 % больше, чем в 2019 году (125 атак). В девяти из десяти атак на промышленность злоумышленники использовали вредоносное ПО. На долю шифровальщиков пришлось 38 % атак, а шпионское ПО было замечено в 30 % случаев.

В начале года внимание многих специалистов по кибербезопасности привлек новый шифровальщик Snake, который умеет удалять теневые копии и останавливать процессы, связанные с работой промышленных систем управления. Первыми жертвами Snake стали автомобильный производитель Honda и гигант ТЭК – компания Enel Group. Сегодня регулярно появляется информация о взломах крупнейших энергетических и производственных компаний по всему миру. Такие атаки сложно скрыть, а определить их источник очень просто: преступники сами сообщают о взломе и требуют выкуп.

С определенной изощренностью в минувшем году злоумышленники нацелились на логические уязвимости в банковских приложениях. Поэтому проявилась положительная динамика по обеспечению безопасности банковских веб-приложений, а именно тенденция к переходу на микросервисную архитектуру, повышающую отказоустойчивость системы, и уменьшение количества стандартных веб-уязвимостей (XSS, SQLi, RCE). Из негативных стоит отметить тенденцию к

увеличению числа логических уязвимостей, которые могут привести к краже денежных средств, получению преступниками дополнительной информации о пользователях, отказу в обслуживании. Таким образом, злоумышленники сейчас нацелены не на полную компрометацию системы банковского веб-приложения, а на логические уязвимости.

По мнению руководителя группы исследований безопасности банковских систем Positive Technologies Максима Костикова, среди возможных негативных сценариев 2021 года эксперты Positive Technologies отмечают прежде всего эксплуатацию темы COVID-19 и новые методы фишинга.

– Мы ожидаем, – говорит Максим Костиков, – что в 2021 году будут совершенствоваться методы социальной инженерии, эксплуатирующие темы, связанные с обстановкой в мире. К примеру, одной из популярных схем могут стать сайты, на которых мошенники будут предлагать заказать препараты для лечения коронавируса, записаться на платную вакцинацию, получить справку о ее прохождении и т. п. Можно ожидать также, что фишинг станет более индивидуальным: злоумышленники будут выходить на жертв через мессенджеры и социальные сети. Для преодоления корпоративных средств защиты взлом все чаще будет производиться через домашние компьютеры работников...

Предполагается определенный рост числа киберпреступных картелей и появление новых площадок в дарквебе. Скорее всего шифровальщики сохранят отработанную в 2020 году стратегию шантажа.

Преступники продолжат атаковать промышленные предприятия и будут ориентироваться на как можно более крупные организации, в то же время предпочитая придерживаться наименьших затрат на взлом или покупку готового доступа в инфраструктуру. Стоит ожидать, что мы услышим о множестве утечек и об остановке производств и в 2021 году: увеличение числа жертв, готовых платить, лишь стимулирует преступников.

Массовая удаленная работа не могла не сказаться на состоянии кибербезопасности как бизнеса и госучреждений, так и обычных пользователей. Социальная инженерия теперь часто применяется для проникновения в сети организаций. Появление новых электронных сервисов обязательно заинтересует преступников и потребует особого внимания с точки зрения ИБ. Выходом из создавшегося цифрового коллапса могут стать специализированные киберполигоны, созданные для тестирования объектов инфраструктуры, сервисов и технологий в безопасной среде, считают эксперты.

– Многие компании пересмотрели свое отношение к удаленному режиму работы, – отмечает Алексей Новиков, директор экспертного центра Positive Technologies. – Если в начале 2020 года организациям пришлось спешно переводить сотрудников на работу из дома, то в 2021 году у них появится возможность сделать работу над ошибками, предусмотреть в бюджете средства на обеспечение защиты, организовать работу с учетом лучших практик ИБ. Сегодня компании не могут игнорировать риски: растет заинтересованность в оценке реальных последствий от возможных киберугроз. Появляется множество площадок, предлагающих провести разного рода учения, и наиболее эффективны киберучения на основе цифровой модели организации, соответствующей реальной инфраструктуре. Моделирование бизнес-рисков на киберполигоне обещает стать одним из основных трендов ИБ в ближайшем будущем.

P.S. В эпоху, когда люди постоянно взаимодействуют через соцсети и мессенджеры, все острее становится вопрос обеспечения их безопасности. Это заставляет сообщество и IT-индустрию более серьезно задуматься о выработке кардинальных подходов к ИБ с дальнейшим их применением на практике в глобальном масштабе. Поэтому в заглавии статьи право поставить знак препинания редакция оставляет за читателями.