а также мер, направленных на обеспечение бесперебойной их работоспособности. Например, использование легального и актуального антивирусного программного обеспечения, шифрование защищаемой информации, применение межсетевых экранов, обновление операционных систем и т. п.;

2. Организационные, т. е. обеспечение физической защищенности информации от ее получения злоумышленниками. Например, постоянное (своевременное, систематическое) обучение обычных пользователей, персонала организаций на предмет информационной безопасности, непренебрежение способами защиты: логины, сложные пароли, иные методы аутентификации, сохранение их в тайне; информирование пользователей о новых видах угроз и способах их реализации; помещение конфиденциальной информации в надежные хранилища и т. д.;

3. Правовые меры, т. е. разработка норм, правил, инструкций, определяющих методы и способы контроля эффективности защиты информации, обозначение ответственности за нарушения. Данная группа относительно эффективна: и уголовное законодательство РФ, и международные документы, и участие РФ в заседаниях международных организаций, которые, в свою очередь, уделяют большое внимание преступлениям в сфере компьютерной информации, киберпреступности и сотрудничеству государств в данной области.

Российской Федерацией признаются существующие проблемы в этой области и ведется следующая работа: в органах исполнительной власти созданы специальные подразделения (например, Управление «К» МВД России, Национальный координационный центр по компьютерным инцидентам, созданный ФСБ России), ведущие борьбу с компьютерными преступлениями; актуализируется законодательство РФ (например, в гл. 28 УК РФ в 2017 г. были внесены изменения, в Доктрине информационной безопасности РФ (указ Президента РФ от 5 декабря 2016 г. № 646) в разд. III компьютерные преступления обозначены как один из видов угроз безопасности страны); подготавливаются кадры для работы в данном направлении (различные учебные заведения); на постоянной основе проводятся дополнительное обучение, переподготовка и повышение квалификации в области информационной безопасности сотрудников различных органов и организаций, а также иная деятельность.

Подводя итог, отметим, что количество совершенных преступлений в сфере компьютерной информации растет, о чем говорят приведенные статистические данные. Происходит это, на наш взгляд, из-за бурного развития информационных технологий, их доступности как для обычного пользователя, так и для преступного элемента. Комплексность подходов по противодействию, борьбе с преступностью и минимизации возможного ущерба от их действий – залог успеха.

УДК 341.23:[343:004.9]

С.А. Чернышева, кандидат технических наук, доцент, профессор кафедры логистики и информационно-математических дисциплин, Минск, БИП – Институт правоведения
s_chernyshova@mail.ru

БОРЬБА С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ – КЛЮЧЕВОЕ ЗВЕНО В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На современном этапе развития информационного общества вопросы информационной безопасности в системе национальной безопасности государства приобретают первостепенное значение и охватывают практически все сферы жизнедеятельности человека.

Компьютерные преступления в контексте информационной безопасности представляют собой противоправные деяния, которые, кроме того, имеют международную природу благодаря устойчивому росту современных средств связи.

В Беларуси количество преступлений в сфере высоких технологий за пять лет стремительно возросло, наметилась устойчивая тенденция к увеличению количества зарегистрированных преступлений в этой сфере.

По данным МВД Республики Беларусь, в 2017 г. было зарегистрировано 3 999 преступлений, в 2018 г. – 4 741, а за 8 месяцев 2019 г. – 5 753 преступления, связанные с IT-технологиями. Такая динамика обусловлена ростом числа зарегистрированных в стране хищений путем использования компьютерной техники и осуществления несанкционированного доступа к компьютерной информации.

В настоящее время борьба с компьютерными преступлениями в сфере высоких технологий требует самого пристального внимания, анализа сложившейся ситуации и принятия конкретных радикальных решений.

Среди мер, направленных на эффективное улучшение ситуации, следует выделить образовательный аспект проблемы, а именно качественную подготовку специалистов нового направления, связанного с обеспечением информационной безопасности.

Так, в Академии МВД Республики Беларусь по инициативе Управления «К» началась подготовка по направлению «Противодействие киберпреступности и компьютерная разведка». Педагоги не только обучают специалистов для Управления «К», но и в целом вооружают сотрудников органов внутренних дел знаниями для борьбы с преступлениями, которые совершаются с помощью информационных техноло-

гий. Уникальный белорусский вуз первым в СНГ так подошел к решению вопроса цифровой грамотности сотрудников органов внутренних дел.

Курсанты новой специальности изучают международно-правовую базу и правовые аспекты информационной безопасности и защиты информации, универсальное и специализированное программное обеспечение, методы совершения преступниками противоправных деяний и т. д.

Основная часть занятий – практическая, проходит за компьютерами, а также в профильных службах ОВД. Курсанты приобретают также углубленные навыки по оперативно-разыскной деятельности в сети.

В свете рассмотренного выше, на наш взгляд, целесообразно включить в учебные планы всех специальностей современного образования, в том числе высшего, актуальную учебную дисциплину «Информационная безопасность и защита информации». Изучение данной дисциплины позволит сформировать у будущих специалистов различного профиля комплекс теоретических знаний, практических умений и навыков в области создания и управления системами информационной безопасности предприятий и организаций.

В заключение следует подчеркнуть, что транснациональность угроз в информационной сфере и уровень ущерба при их реализации ставят проблему обеспечения информационной безопасности как глобальную, требующую усилий всего мирового сообщества.

Государства мира уже давно осознали необходимость сотрудничества в борьбе с компьютерными преступлениями: принята Европейская конвенция о киберпреступности 2001 г., подписано Соглашение о сотрудничестве государств СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 г., создана Международная специализированная организация по борьбе с кибертерроризмом «ИМПАКТ».

Однако проблемы единого подхода к киберпреступности остаются. Необходима разработка единых международных стандартов по юридическим, процессуальным и процедурным вопросам, которые позволяли бы классифицировать те или иные нарушения и принимать адекватные меры для их пресечения.

Выход из данного положения видится в заключении универсальной Конвенции по борьбе с киберпреступностью, разработке и подписании региональных договоров.

Усилия мирового сообщества должны быть направлены на разработку реальной стратегии интеграции в рамках глобального информационного общества.

УДК 378:004.9

Е.В. Чистая, преподаватель кафедры правовой информатики Академии МВД Республики Беларусь
843062@mail.ru

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ СРЕД В УЧРЕЖДЕНИЯХ ВЫСШЕГО ОБРАЗОВАНИЯ В СООТВЕТСТВИИ С БОЛОНСКОЙ ДЕКЛАРАЦИЕЙ

В современном обществе наиболее актуальной становится подготовка специалиста, обладающего не только крепкими теоретическими знаниями, но и устойчивыми практическими навыками, для эффективной практической деятельности.

19 июня 1999 г. была подписана Болонская декларация, признанная урегулировать процесс сближения стран Европы в сфере высшего образования. В ней говорится: «Жизнеспособность и эффективность любой цивилизации обусловлены привлекательностью, которая ее культура имеет для других стран. Мы должны быть уверены, что европейская система высшего образования приобретает всемирный уровень притяжения, соответствующий нашим экстраординарным культурным и научным традициям». Россия присоединилась к Болонскому процессу в сентябре 2003 г. на берлинской встрече министров образования европейских стран. В 2005 г. в Бергене Болонскую декларацию подписал министр образования Украины. 14 мая 2015 г. в Ереване на Конференции министров образования стран ЕПВО и форуме по Болонской политике было объявлено о присоединении Белоруссии к Болонскому процессу и вступлении ее в Европейское пространство высшего образования. Одной из основных целей Болонского процесса является «содействие мобильности путем преодоления препятствий эффективному осуществлению свободного передвижения». В значительной мере этому будет способствовать унификация выдаваемых дипломов о высшем образовании, сходность специальностей и специализаций модульной системы образования, приведение к общим правилам перезачета сходных дисциплин.

Компьютерные сети и сети Интернет позволяют реализовать данные новшества в качестве модульной образовательной среды. Нужно обратить внимание на необходимость мультиязыковых сред для реализации электронных материалов. Реализация должна проходить не только на национальных языках, но и синхронизирована со странами, участвующими в Болонском процессе.

Особенно актуальной является не столько аккумуляция теоретической информации, сколько унификация между разными странами педа-