

криминальной полиции. По их данным, более 22 % сотрудникам вообще никогда не оказывалось сопротивление, что, по мнению специалистов, связано с непродолжительным сроком службы в полиции. Вместе с тем 78 % сотрудникам полиции при выполнении служебно-оперативных задач, связанных с преследованием и задержанием правонарушителей, оказывалось сопротивление, им приходилось вступать в рукопашные схватки, а также использовать табельное оружие. При этом авторы отмечают, что 34,4 % опрошенных испытывали растерянность при возникновении необходимости применить оружие, 22,1 % респондентов указали на боязнь стрельбы в правонарушителя.

В аспекте нашей профессиональной специализации особенный интерес вызывает характер защитно-ответных действий, применяемых сотрудниками полиции в рукопашных схватках при преследовании и задержании правонарушителей. Защита от ударов руками, ногами и подручными средствами использовалась сотрудниками в 52 % случаев. Из видов защитных приемов и действий полицейские наиболее часто использовали уходы (65 %), подставки (48 %) и уклоны (54 %). Ответные действия руками и ногами применяли 63 % опрошенных. При этом большинство респондентов считают, что более эффективными ударами являются удары руками и удары ногами на нижнем уровне. Непосредственно задержание осуществляется как в положении лежа, так и в положении стоя (28 %), при этом наиболее часто применяется «загиб руки за спину». В то же время при угрозе огнестрельным оружием большинство сотрудников предпочитают не приемы защиты, а уход из сектора поражения в сочетании с ударами руками и с последующим задержанием (31 %).

В настоящем исследовании приняло участие 136 респондентов (участковые инспектора милиции, сотрудники департамента охраны, оперативно-дежурной службы, патрульно-постовой службы милиции, уголовного розыска, изолятора временного содержания, отряда милиции особого назначения) в основном возрасте от 20 до 35 лет со средним стажем работы от 5 до 15 лет. По результатам анкетирования было установлено, что более половины опрошенных (56,2 %) вступали в противоборство с правонарушителями за период службы более пяти раз, 27,4 % – до пяти раз и только 14,1 % из числа опрошенных указали на то, что им еще не приходилось в своей служебной деятельности применять приемы самообороны. Как показывает практика, вариативность атак нарушителей достаточно велика. В большинстве своем ими используются: палки – 37 % случаев, ножи – 31,2 %, камни – 9,3 %, топоры – 1,3 %, и другие виды подручных средств и оружия. При этом удары занимают ведущее место – 67,3 %, в меньшей степени применяются приемы борьбы – 17,5 %, броски – 5,2 %, а также болевые приемы – 2,9 %. Большой практический интерес представляет также анализ способов защиты от непосредственного удара и нападения. Большинство респондентов считают, что уходы (33,8 %), блоки (38,2 %), уклоны (31,9 %) и упреждающие удары (44,3 %) являются наиболее эффективными способами защиты в опасных ситуациях. Наиболее типичными местами проведения задержания правонарушителей являются улица – 72,3 % респондентов, подъезды домов – 23,4 %, в меньшей степени общественные учреждения – 11,3 % и транспорт – 12,3 %, менее часто задержания производятся в квартире – 4,4 %.

Таким образом, изучение и знание типичных ситуаций противоборств с правонарушителем позволяет корректировать и соответственно совершенствовать процесс технической подготовки сотрудников и соответственно обеспечивать готовность их к действиям в реальных ситуациях силового задержания.

УДК 343.982.067

*В.Е. Козлов*

### **ЗАКЛАДНЫЕ ЭЛЕМЕНТЫ КАК КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ИЗ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ**

Широкое обсуждение в средствах массовой информации возможностей использования каналов утечки информации (КУИ) из средств компьютерной техники (СКТ), инициированное «разоблачениями» бывшего сотрудника Агентства национальной безопасности (NSA) США Э. Сноудена, и их использование для достижения контроля над информационными системами различных субъектов, требует упорядочения знаний, накопленных в теории и практике противодействия высокотехнологичной преступности.

КУИ – совокупность источников информации, материальных носителей или среды распространения, несущих эту информацию, а также средств выделения информации. КУИ из СКТ на объекте безопасности относятся к так называемым частным каналам утечки. Они возникают при осуществлении внедрения и использования специфических средств и технологий обработки информации в рассматриваемой предметной области – компьютерной информации (КИ). Таким образом, частные КУИ, характерные только для СКТ, выделены в процессе широкого внедрения и использования таких средств и технологий. В зависимости от применяемых технологий внедрения и эксплуатации КУИ из СКТ классифицируются следующим образом.

Программные закладные элементы (ЗЭ) – внедренные программы либо их измененные фрагменты (код), позволяющие реализовать угрозу КИ вследствие изменений свойств систем защиты СКТ.

Аппаратные ЗЭ – устройства, предназначенные для перехвата КИ, скрыто внедряемые в СКТ, либо сети передачи КИ, позволяющие реализовать угрозу КИ вследствие изменений свойств систем защиты СКТ.

Классификация ЗЭ также может быть проведена по различным основаниям: по объекту воздействия; методам (способам) активизации и сокрытия; времени начала работы; способу управления и получения КИ и т. д. Достаточно широкое использование ЗЭ со стороны криминала и специальных служб иностранных государств является следствием как минимум двух обстоятельств. Во-первых, выраженной зависимостью производства СКТ и программного обеспечения (ПО) от комплектующих изделий зарубежного производства. Такой подход обеспечивает конкурентоспособность выпускаемых изделий, однако, при этом появляется угроза утечки КИ, а также управляемого выведения из строя СКТ, заложенная в них либо на этапе производства (сборки), либо при иных обстоятельствах в процессе эксплуатации. Во-вторых, значительным повышением криминальной квалификации субъектов, совершающих высокотехнологичные преступления, причем существует реальная возможность «повышения данной квалификации» путем обмена опытом на специализированных форумах и в социальных сетях.

Использование ЗЭ является реальной угрозой при использовании СКТ, так как они способны обеспечить выполнение, например, следующих задач: установление и выдачи точного местоположения элементов систем обработки КИ; их скрытое дублирование; внесение изменений в коды и алгоритмы работы различного ПО; навязывание определенных режимов или алгоритмов

работы СКТ; умышленное искажение передаваемой КИ; доступ к КИ в обход средств защиты; влияние на здоровье, психику, и, как следствие, поведение обслуживающего персонала – так называемая оперативная рефлексия (социальная инженерия). Например, некто А., являясь инженером-программистом первой категории одного из минских УП, с целью несанкционированного уничтожения КИ, разработал ПО. Находясь в служебном помещении УП, с использованием СКТ и установленного на нем ПО скомпилировал исполняемый модуль ПО, назвав его *Simen.exe*. А. установил копии названного исполняемого модуля в системные каталоги операционной системы (ОС) Windows на жесткие диски сети УП. Для каждого СКТ было установлено различное время начала уничтожения КИ. В результате были уничтожены следующие программные комплексы: «Складской учет», «Заведующая секцией», вспомогательное ПО, базы данных о движении материальных ценностей, а также поврежден BIOS. В последующем установлено, что мотивом совершения данного преступления явились неприязненные отношения А. со своим непосредственным руководителем – начальником отдела АСУ УП некой Б.

Количество таких примеров, различающихся средствами совершения либо мотивами, велико. Положительную динамику имеет также совершение хищений из банкоматов белорусских банков, совершаемых с использованием ЗЭ. В этом случае, речь идет об использовании скиммеров (накладок), либо механических блокираторов банковских платежных карт (так называемые ливанские петли). По данным МВД Республики Беларусь, количество хищений, совершаемых по линии борьбы с преступлениями в сфере высоких технологий за 2013 г. составило 89 % от общего их количества (2558), увеличившись на 25,4 %.

Следует отметить, что установка ЗЭ в СКТ может являться одним из технических приемов при ведении т «информационных войн» – в этом случае ЗЭ рассматриваются в качестве информационно-программного оружия, в результате применения которого в необходимый момент управление критичными объектами безопасности государства может быть нарушено либо утрачено.

Борьба с высокотехнологичной преступностью является одной из наиболее актуальных задач правоохранительных органов Беларуси. Для повышения ее эффективности целесообразна реализация комплексных мер, рассматриваемых по двум направлениям.

Во-первых, непрерывное повышение квалификации сотрудников органов внутренних дел. Причем речь идет не столько о сотрудниках специализированных оперативных, экспертных и следственных подразделений, сколько об иных сотрудниках, прежде всего низовых подразделений. В этом смысле, целесообразно интенсифицировать процессы овладения новыми знаниями путем проведения семинаров (в том числе выездных), специальных курсов, преподаваемых в период повышения квалификации либо переподготовки (например «Технические средства оперативно-розыскного назначения», «Технические средства охраны общественного порядка и обеспечения безопасности», «Организация применения криминалистической и специальной техники», преподаваемых по кафедре тактико-специальной подготовки Академии МВД Республики Беларусь), практических тренингов. Следует также определить необходимый и достаточный минимум знаний в области высоких технологий, который может быть использован названными сотрудниками в процессе исполнения ими своих должностных обязанностей.

Во-вторых, необходимо постоянно совершенствовать процесс информирования граждан и должностных лиц о новых способах совершения преступлений, мерах обеспечения безопасного использования новых технологий обработки КИ. Речь идет прежде всего об использовании средств массовой информации, тематических сайтов интернета. Эффективными также следует признать семинары, проводимые совместно с сотрудниками, работающими в банковской, финансовой и иных сферах (например, работниками предприятий, оказывающими услуги сотовой подвижной электросвязи). В этом случае тематика проводимых занятий уточняется в соответствии с категориями обучаемых (руководители, ИТ-специалисты, юристы, операторы, пользователи).

УДК 796.015.132

*В.П. Лашкин, Д.В. Панцевич*

### **СПОРТИВНЫЕ ИГРЫ В ПРОФЕССИОНАЛЬНО-ПРИКЛАДНОЙ ФИЗИЧЕСКОЙ ПОДГОТОВКЕ КУРСАНТОВ УЧРЕЖДЕНИЙ ОБРАЗОВАНИЯ МВД РЕСПУБЛИКИ БЕЛАРУСЬ**

В любых профессиях профессиональный рост будущего специалиста подразумевает развитие его физической культуры. Будучи совокупностью физических и психических качеств человека, физическая культура является жизненной и профессиональной его потребностью. Сегодня наибольшее теоретическое освещение прикладности физической культуры имеет профессионально-прикладная физическая подготовка (ППФП) как сложившаяся форма ее проявления. ППФП – специализированный педагогический процесс с применением определенных форм, средств и методов физического воспитания, которые в оптимальной степени обеспечивают развитие и совершенствование психических и физических качеств, двигательных навыков и функций организма в соответствии с требованиями той или иной профессии. Более того, основоположник теории и методики физического воспитания и спортивной тренировки профессор Л.П. Матвеев, отмечая важность ППФП в профессиональном становлении военнослужащих силовых ведомств, впервые дал определение ППФП сотрудников органов внутренних дел.

Особую актуальность ППФП приобретает в отношении профессионального образования будущих офицеров органов внутренних дел – курсантов учреждений образования МВД Республики Беларусь, потому что профессиональная подготовленность офицерского состава милиции является решающим фактором обеспечения законности, правопорядка и борьбы с преступностью. ППФП – один из немногих предметов, преподавание которого осуществляется на протяжении всего периода обучения. Она является составной частью учебного процесса и ставит целью в ходе проведения теоретических и практических занятий и соревнований обеспечить психофизическую готовность курсантов к будущей профессиональной деятельности.

Большое значение в освоении прикладных умений и навыков, воспитании психофизических качеств имеет направленный подбор эффективных средств, которыми можно акцентировано воздействовать на курсантов, способствуя формированию у них конкретных психофизических качеств и свойств личности, определяющих успешность будущей профессиональной деятельности. Программа по ППФП предполагает взаимосвязанное использование видов физических упражнений, которые оказывают как общее развивающее воздействие, так и специальное (относительно к профессиональной деятельности). Для решения этих задач используются средства профессионально-прикладных видов спорта (рукопашный бой, самбо, самозащита без оружия, служебное многоборье). На наш взгляд, из-за недостаточной избирательности и неполного охвата задач, которые должна решать