

НЕКОТОРЫЕ АСПЕКТЫ ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНОГО САБОТАЖА

Термин «саботаж» (от фр. sabot – башмак) возник как название акции, к которой прибегали французские рабочие – мельники в начале XIX в. Когда вспыхивал трудовой конфликт, они с помощью своих башмаков останавливали мельницы, на которых молотило зерно.

В УК РСФСР 1926 г. саботаж относился к «контрреволюционным преступлениям» (ст. 58) и определялся как «сознательное неисполнение кем-либо определенных обязанностей или умышленное небрежное их исполнении со специальной целью ослабления власти правительства и деятельности государственного аппарата».

Развитие научно-технического прогресса явилось одним из факторов, оказавшим влияние на качественные изменения преступности. Автоматизированные системы управления, электросвязи, мониторинга, прогнозирования, охраны объектов и имущества, а также средства их обеспечения, конструктивно выполненные на базе разнообразных микропроцессорных устройств, стали неотъемлемой частью высокодоходных и денежнооемких технологий, используемых в стратегических сферах хозяйства и обороны страны. Все это в совокупности с широкими возможностями и доступностью средств компьютерной техники и телекоммуникаций, обезличенностью основной части содержащейся в них компьютерной информации привлекает внимание злоумышленников.

Информатизация современного общества привела к формированию новой формы саботажа – компьютерного, при совершении которого используются современные информационные технологии, новейшие средства телекоммуникации и связи.

Компьютерный саботаж в уголовном праве Республики Беларусь определен как умышленное уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (ст. 351 Уголовного кодекса Республики Беларусь).

Согласно данным международного комитета по компьютерной преступности, занимающегося исследованиями масштабов и видов компьютерных преступлений, а также правовыми аспектами борьбы с этим видом преступности, компьютерный саботаж представляет собой серьезную угрозу для любой располагающей компьютерной техникой организации. Например, вывод из строя управляющей автоматизированной информационной системы в результате данного преступления может нанести даже самой крупной компании за короткое время значительный материальный ущерб. Поскольку деятельность многих современных предприятий очень сильно завязана на непрерывном функционировании информационной инфраструктуры, саботажники способны нанести удар по самым уязвимым точкам информационной системы, уничтожив, например, критические данные на серверах и в резервных копиях.

Первое уголовное дело в Республике Беларусь, возбужденное по ст. 351 «Компьютерный саботаж» Уголовного кодекса Республики Беларусь, было заведено в 2005 г. в отношении работников областного отделения Белорусской железной дороги. Один из руководителей и инженер-технолог вагонного депо самовольно решили внести изменения в базу данных централизованной информационной системы Белорусской железной дороги. В результате была уничтожена компьютерная программа, из-за чего доступ к обслуживанию сервера всего Витебского отделения дороги оказался заблокированным. Последствия могли быть очень серьезными: от потери данных и важной информации, вывода из строя и полного разрушения локальной компьютерной сети до нарушения графиков движения и полной остановки транспортных средств.

Компьютерный саботаж является одной из наиболее опасных угроз в сфере информационной безопасности. В центре такого инцидента, как правило, всегда находится служащий компании, инсайдер – человек, знающий слабые стороны организации изнутри и прекрасно представляющий, что именно нужно сделать, чтобы нанести работодателю максимальный ущерб.

Отличие компьютерного саботажа от обычных внутренних угроз информационной безопасности состоит в тех мотивах, которыми руководствуется инсайдер в своих противоправных действиях. Как правило, им движет злость, месть, обида, желание доказать собственную значимость, реже – корысть и личная выгода. Многие коммерческие компании стараются всячески скрыть подобные инциденты от общественности, совершенно справедливо полагая, что акционерам, инвесторам, партнерам и клиентам компании вряд ли понравится тот факт, что в корпорации возможны столь острые конфликтные ситуации, развязка которых приводит к серьезным финансовым убыткам.

Рассмотрим характерные черты типичного саботажника.

Как показало исследование Российского центра реагирования на компьютерные инциденты (CERT), в 98 % случаев инициатором компьютерного саботажа являлся мужчина, которым в 84 % случаев двигало желание отомстить. Несколько реже (24 %) инсайдеры хотели выразить несогласие с политикой компании и еще реже (12 %) хотели быть оценены по достоинству. Правда, в более чем половине всех случаев (57 %) саботажником двигали сразу несколько мотивов.

Отметим, что все эти мотивы являются лишь реакцией на события, произошедшие ранее. В 92 % случаев компьютерному саботажу предшествует неприятный инцидент или целая серия таких инцидентов на работе. В 47 % случаев – увольнение, в 20 % – спор с нынешними или бывшими коллегами, в 13 % – понижение в должности или отсутствие повышения. Другими словами, 85 % всех внутренних диверсантов рассержены на кого-то, кого они ассоциируют с компанией.

Еще одной очень важной деталью портрета компьютерного саботажника является его профессиональная принадлежность. Как показало исследование CERT, почти все корпоративные диверсанты являются специалистами, так или иначе связанными с информационными технологиями. Среди них 38 % системных администраторов, 21 % программистов, 14 % инженеров, 14 % специалистов в области информационной безопасности. На долю этих специалистов приходится 86 % инцидентов. Сказанное позволяет полагать, что движущая сила угрозы компьютерного саботажа лежит в области человеческих отношений. Однако на практике можно существенно минимизировать риски данного преступления.

Изучение дел данной категории показало, что проблемные служащие несут ответственность за 80 % всех внутренних компьютерных инцидентов. Следовательно, одной из мер минимизации рисков компьютерного саботажа является заблаговременное выявление наиболее проблемных инсайдеров.

Следует заметить, что проблемные сотрудники не только осуществляют 80 % всех атак, но в 62 % случаев планируют свои действия заранее. Тем не менее существует ряд признаков, по которым можно выявить инсайдеров: они жалуются на

свою зарплату, опаздывают или прогуливают, эмоционально спорят с коллегами, нарушают субординацию, ведут себя агрессивно. Перечисленные элементы поведения следует учитывать в комплексе, так как по отдельности они могут наблюдаться даже у самых лучших сотрудников фирмы. Если руководству компании удалось выявить служащих, которые удовлетворяют описанному выше шаблону, то действия этих инсайдеров следует тщательно контролировать, а также желательно ограничить полномочия таких пользователей при доступе к информационной системе.

В целом использование этих рекомендаций позволяет в большинстве случаев предотвратить компьютерный саботаж в корпоративной среде и избежать значительных финансовых убытков.

УДК 343.43

Я. Брык

УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ ТОРГОВЛИ ЛЮДЬМИ

Торговля людьми лишает людей их прав и свобод, представляет собой глобальную угрозу для их жизни и здоровья, является одной из форм организованной преступности. Она влияет не только на отдельных людей, которые становятся ее жертвами, но и снижает безопасность, качество социального обеспечения, общественный порядок всех наций, которых она касается. Борьба с торговлей людьми является одной из наиболее важных задач, стоящих сегодня перед международным сообществом. Размер этого явления показывает, что XXI в. не является свободным от рабства и принудительного труда.

Торговля людьми – не новое явление, характерное только для современной действительности. В качестве проблемы ее начали рассматривать в более широком, чем местный, масштабе в конце XIX в., когда в 1899 г. в Лондоне прошел первый Международный конгресс по торговле белыми рабами. Тогда международное сообщество начало сотрудничество в борьбе с этим явлением, которое более или менее интенсивно продолжается по сей день. Результатом сотрудничества на правовой основе являются многочисленные правовые договоры международного характера.

Торговля людьми начала принимать угрожающие масштабы в 90-х гг. XX в. Причиной этого, несомненно, были социально-экономические и политические изменения, происходящие в Европе, особенно в странах Центральной и Восточной Европы, открытие границ, безработица, и то, что происходит вместе с ними – миграция населения. Эти процессы заинтересовали не только мелких преступников, но и организованные преступные группы, сфера действий которых раньше была сосредоточена вокруг незаконного оборота наркотиков, оружия или произведений искусства. В настоящее время торговля людьми является третьим после наркотиков и оружия источником дохода международных преступных групп.

Точное число людей, которые становятся жертвами торговли людьми, определить невозможно. Данные, которые приводят определенные организации или учреждения, – приближенного, ориентировочного характера и не отражают реального положения дел. Наиболее важной причиной этого представляется то, что о случае торговли знают преступники и жертвы, которые, будучи иногда единственными свидетелями преступления, из-за незнания, стыда или страха не принимают дальнейших мер по разоблачению преступников.

Торговля людьми включает в себя сексуальное использование, использование для работы в условиях, близких к рабству, детскую порнографию, торговлю органами, попрошайничество.

Жертвы торговли людьми подвергаются насилию и особо жестокому психическому давлению, принуждению, запугиванию.

Наиболее распространенное и одновременно наиболее изученное явление – торговля женщинами в целях проституции. Широкие круги охватывает торговля детьми в целях их сексуальной эксплуатации.

Анализ текущего состояния преступности, проведенный на основе предварительного расследования, указывает на изменение роли Польши в торговле людьми. Польша больше не является страной происхождения, а становится транзитной страной, через которую перебрасываются женщины в основном из бывшего Советского Союза и Восточной Европы. В настоящее время более четко можно увидеть следующий этап трансформации данного явления. Это «импорт людей», а Польша выступает в качестве страны назначения. Организованные преступные группы, специализирующиеся на торговле людьми, «приобретают» женщин из Болгарии и стран бывшего Советского Союза, африканских стран для сексуальных услуг в секс-агентствах, массажных салонах, а также на дорогах.

В дополнение к территориальному аспекту торговли людьми в Польше отметим также субъектный аспект, указывающий на участие польских граждан в торговле людьми за пределами Польши. В настоящее время мы имеем дело с торговлей людьми для рабского труда в лагерях на юге Италии и Испании. Это типичный пример. Часто это дело большой международной уголовной организации, действующей как в Польше, так и за рубежом. К наиболее дерзким преступлениям принадлежат раскрытые случаи торговли детьми для незаконного усыновления. Польша выступает в качестве страны происхождения жертв-детей. Польские граждане за рубежом также очень активны в осуществлении этого вида преступления.

Торговля людьми была признана преступлением в Польше уже в межвоенный период. Свидетельством этого является ратификация Польшей первых международных правовых документов в этой области, а также пенализация определенного поведения в Уголовном кодексе. Следует отметить, что в доктрине уголовного права в межвоенный период торговля людьми неразрывно связана с явлением проституции, что соответствовало духу тогдашних международно-правовых документов. Такой подход также отражен в первой польской кодификации – Уголовном кодексе 1932 г.

В действующем Уголовном кодексе Польши 1997 г. законодатель поместил правовое положение, касающиеся торговли людьми, в ст. 189а, хотя определение «торговля людьми» выступает как понятие в § 22 ст. 115.

Торговля людьми включает вербовку, перевозку, передачу, укрывательство людей путем:

- 1) насилия или угрозы;
- 2) похищения;
- 3) обмана;
- 4) введения в заблуждение, использования ошибки или неспособности к правильному пониманию данного действия;
- 5) использования критического положения или состояния беспомощности;