PolotskSU

Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

PolotskSU

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

© Полоцкий государственный университет», 2017

PolotskSU

туализации (например, в случае VMware vSphere функция кластера High Availability). Таким образом, в случае сбоя сервера восстановить работоспособность комплекса не составит труда. В случае работы с микрокомпьютером для резервирования достаточно приобрести дополнительный МК.

Вторая сущность, которую необходимо продублировать – МНЛ. Нельзя просто так дать пользователю резервную копию устройства, которое может генерировать лицензии: необходимо защитить продавца от неправомерного использования покупателем резервных устройств для удвоения доступных лицензий. Для этого предлагается использовать 3 типа устройств: одно выписывающее, одно дублирующее и набор пустых. Выписывающее и дублирующее устройства работают только в паре на одном сервере. Выписывающее устройство генерирует лицензию только с разрешения дублирующего. Число лицензий уменьшается на обоих устройствах. В случае, если одно устройство выходит из строя, при помощи оставшегося в рабочем состоянии и пустого устройства создаётся замена сломанному. Если у пользователя окажется 2 пустых устройства (а минимум два ему необходимы т.к. выписывающее и дублирующее работают одновременно, соответственно и ресурс у них исчерпывается идентично), то он сможет сделать второй комплект. Чтобы избежать этого предлагается устанавливать на пустые устройства пин-коды, которые будут предоставляться пользователю по факту обращения (при этом пользователь обязан будет вернуть вышедшее из строя). Таким образом, покупатель не сможет использовать одно из дублирующих устройств отдельно и не сможет создать две рабочих пары.

Выводы. Предложенная схема позволяет упростить процесс установки, решить вопрос с отзывом и уменьшить время развертывания программных комплексов, что особенно важно для больших информационных систем. Она не привносит уязвимостей в схему оригинального мобильного носителя лицензий, так как решения о выписывании лицензий по-прежнему принимаются внутри устройства, но сильно расширяет его возможности и делает процесс быстрее и удобнее.

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

И.Т. ЧЕРНЕНКО

Управление по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Республики Беларусь,

Первое высокотехнологичное преступление на территории нашей республики было зарегистрировано в г. Минске 20 ноября 1998 года. Внедрив в программное обеспечение «компьютера-жертвы» вредоносную программу типа «троянский конь» под названием «BackOrifice», злоумышленник осуществил несанкционированный доступ к сетевым реквизитам пользователей сети Интернет, из числа клиентов крупнейшего на то время в Беларуси столичного сервис-провайдера «OpenBy», после чего продавал их третьим лицам.

В 2001 году руководство МВД проанализировало криминогенную обстановку, складывающуюся в сфере компьютерной информации и телекоммуникаций в нашей стране, а также странах дальнего и ближнего зарубежья. При этом была изучена организация работы правоохранительных органов других государств по предупреждению и раскрытию преступлений данной категории, опыт борьбы с киберпреступностью российских коллег.

PolotskSU

Принимая во внимание правонарушения, зарегистрированные в 1998–2001 годах, вступление в действие нового Уголовного кодекса, предусматривающего ответственность за преступления против информационной безопасности, а также высокую степень вероятности дальнейшего распространения киберпреступности на территории нашей страны, 28 ноября 2002 г. Министром внутренних дел было принято решение о создании подразделения, специализирующегося на профилактике и раскрытии преступлений данной категории.

Им стало управление по раскрытию преступлений в сфере высоких технологий (далее - УРПСВТ) Министерства внутренних дел Республики Беларусь (далее - МВД). Управление является самостоятельным оперативно–розыскным подразделением МВД. Для осуществления взаимодействия с иными правоохранительными органами и организациями применяется условное наименование «Управление «К» МВД Республики Беларусь.

Управление определено головным подразделением в системе органов внутренних дел, отвечающим за организацию борьбы с преступлениями, предусмотренными статьями 212, 349 – 355 Уголовного кодекса Республики Беларусь (хищения путем использования компьютерной техники и преступления против информационной безопасности).

Спустя два года (в 2004 году), которые полностью подтвердили правильность принятого решения, во всех УВД облисполкомов также были созданы отделы криминальной милиции по раскрытию преступлений в сфере высоких технологий.

Результат не заставил себя долго ждать.

Если за три года (1998—2000-й) было возбуждено всего три уголовных дела, связанных с использованием компьютерных технологий, то в период с 2001 по 2005 годы - уже 1813 таких дел.

А за последние 5 лет (с 2012г. по 2016г.) в республике было зарегистрировано 11799 преступлений в сфере информационных технологий.

Рассматривая структуру таких преступлений, следует отметить, что большинство из них составляют хищения путем использования компьютерной техники (ст.212 УК РБ).

Так, в период с 2012 по 2016 гг. было выявлено 10097 таких преступлений, в том числе в 2016 г. - 1820, что составляет 73,7% (*в 2015 – 83,4%*) от общего числа выявленных преступлений по линии СВТ в прошлом году.

Вместе с тем, анализ показывает, что за прошедшие пять лет спектр преступлений в сфере информационных технологий значительно расширился и вышел за рамки правонарушений, имеющих исключительно экономический подтекст. Все чаще стали выявляться хакерские «атаки» на различные интернет-ресурсы. В этот же пятилетний период, число выявленных преступлений против информационной безопасности (ст.ст. 349-355 УК РБ) ежегодно возрастало и составило – 1702, в том числе в 2016 г. - 651 преступление, что составляет 26,3% от общего числа выявленных в прошедшем году киберпреступлений. Для сравнения: в 2012 г. было выявлено 112 таких преступлений.

По статистике, наибольшее количество преступлений рассматриваемого вида ежегодно выявляется в г. Минске. Поэтому, по инициативе МВД, в 2016 году, в ГУВД Минского горисполкома создано управление по раскрытию преступлений в сфере высоких технологий криминальной милиции, а во всех районных управлениях внутренних дел города – группы по раскрытию таких преступлений. Таким образом, сегодня органы внутренних дел столицы значительно укрепили свои возможности в борьбе с киберкриминалом.

Среди особенностей оперативной обстановки в 2016 году можно отметить выявление и раскрытие ряда резонансных хищений с использованием компьютерной техники, поддельных платежных карт, а также фактов блокирования работы программ на компьютерах пользователей с использованием различных вирусов с целью вымогательства денеж-

PolotskSU

ных средств. Задержаны и привлечены к уголовной ответственности организаторы и активные участники шести преступных групп, специализировавшиеся на использовании «скиммеров» (2 группы) и вирусов «блокировщиков» (4).

Некоторые примеры из практики.

В начале 2016 года проводились мероприятия по установлению личностей преступников, которые с использованием поддельных банковских карт на территории г.Минска, г.Могилева и г.Гомеля в январе 2016 года совершили хищение денежных средств на сумму свыше 570 миллионов белорусских рублей. Установлено, что данные преступления совершили двое граждан Российской Федерации, которые были задержаны в г. Воронеже российскими правоохранительными органами. У них изъято оборудование для изготовления поддельных платежных карт, а также более 150 карт с ложными идентификационными логотипами иностранных банков с информацией на магнитной полосе со счетов граждан США и Пуэрто-Рико.

В августе 2016 года в Управление «К» МВД поступило обращение из одного банка по факту обнаружения при вскрытии банкоматов недостачи денежных средств в белорусских рублях и иностранной валюте (527 тыс. долларов США, 67500 евро и более 108 тыс. белорусских рублей). Хищения осуществлялись из 27 банкоматов банка, находящихся в Минске, Могилеве, Витебске. Преступники получили несанкционированный доступ к серверам банка, в том числе к серверу управления банкоматами, что дало возможность осуществить хищения. В результате проведения комплекса ОРМ установлена причастность к хищениям граждан Украины, России и Молдовы.

Некто гражданин «П», находясь в Республике Беларусь и Российской Федерации, в период с января 2013 года по апрель 2014 года, действуя умышленно, в составе организованной группы, из корыстной и иной личной заинтересованности, осуществил сопровождающийся нарушением системы защиты несанкционированный доступ к информации, хранящейся в компьютерной системе финансовой компании (банковского учреждения) «AmericanExpress» (США), в том числе к сведениям не менее 57 карт-счетов держателей банковских платёжных карт, а также к иным конфиденциальным и персональным данным держателей и эмитента (AmericanExpress) указанных карт, без их ведома и согласия. По всем указанным преступлениям возбуждены уголовные дела.

Активные действия белорусских правоохранителей стали предметом внимательного изучения далеко за границами нашей республики. Появление нового «игрока» в мировом киберпространстве не ушло как от пристальных взоров «антихакеров» других стран, так и от IT-злоумышленников всех мастей. Определенные успехи белорусов успокоили первых, так как в рядах профессионалов явно прибыло, и по тем же причинам взволновало вторых.

Так, в 2016 году в результате проведенных ОРМ подразделениями РПСВТ установлено 966 лиц, причастных к их совершению. К уголовной ответственности привлечено 866 человек, в том числе 286, имеющих судимость, 648 неработающих и 34 несовершеннолетних. Последнее изыскание опровергает бытовавшее мнение о том, что такие «проделки», в подавляющем большинстве случаев, совершаются детьми.

На основании вышеприведенного анализа видно, что киберпреступления – удел взрослых, уже сформировавшихся личностей, выбравших вполне осознанно модель своего поведения в обществе.

За годы борьбы с высокотехнологичными преступлениями наш опыт не только восприняли, но и стали перенимать. Сегодня рассмотрение белорусского опыта в рамках различных международных семинаров и конференций является неотъемлемой частью данных мероприятий.

PolotskSU

Начиная с 2009 года, представители управления ежегодно принимают участие в работе Международного конгресса по проблемам борьбы с компьютерной преступностью, проходящего в Лондоне по инициативе Национального комитета по борьбе с преступностью в сфере высоких технологий Великобритании.

Также стали регулярными рабочие встречи в рамках инициативы Совета Европы «Восточное партнерство», российского «Инфофорума» и с руководителями управления «К» МВД Российской Федерации. Последние направлены на обмен опытом и совершенствование механизма взаимодействия.

Практическое международное сотрудничество управления «К» МВД Республики Беларусь по обмену информацией в рамках противодействия киберпреступности осуществляется посредством международной сети Национальных контактных пунктов (НКП), функционирующей в настоящее время под эгидой Римско-Лионской подгруппы «Группы Семи». Римская/Лионская группа – это рабочий орган «Группы семи», который специализируется на проблематике противодействия терроризму и транснациональной организованной преступности. В настоящее время указанная международная сеть национальных контактных пунктов имеется в 70 странах, среди которых Беларусь, Россия, Украина, ФРГ, Великобритания, США, Испания, Швеция, Бразилия и многие другие.

Полноправным членом международной сети НКП управление «К» МВД Беларуси стало в 2008 году по приглашению управления «К» МВД Российской Федерации. Так, на заседании экспертов Римско-Лионской подгруппы, проходившей 9-11 декабря 2008 года в г. Киото (Япония), было единогласно принято решение о вступлении МВД Беларуси в международную сеть НКП.

Оглядываясь на пройденный путь, сегодня можно с уверенностью сказать, что подразделения по раскрытию преступлений в сфере высоких технологий органов внутренних дел Республики Беларусь представляют собой современные, хорошо оснащенные подразделения, способные во взаимодействии с иными правоохранительными органами, решать сложные задачи по противодействию киберпреступности в стране.

Конечно, процесс формирования оперативной, следственной, экспертной и судебной практики применения действующего уголовного законодательства в сфере противодействия киберпреступности пока еще не завершен, но не надо забывать, что это именно та область криминалистики, где постижение нового, еще не изученного – процесс перманентный.

НЕКОТОРЫЕ ВОПРОСЫ ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В.Э. ЯСКЕВИЧ

Государственное учреждение «НТЦ КГБ Республики Беларусь»

В Белорусском государственном университете на факультете радиофизики и компьютерных технологий с 2011 года проводится подготовка специалистов по курсу «Технические средства и методы защиты информации». Опыт преподавания указанной дисциплины, проблемы, достижения и результаты предлагается обсудить в настоящем докладе.

Дисциплина "Технические средства и методы защиты информации" - научно-практическая учебная дисциплина, в которой изучаются вопросы, связанные с форми-