the purchase. Here you can listen to telephone conversations, save an important document, invoice in one click, write an e-mail, set yourself a reminder - for example, prepare a commercial offer. The possibilities of CRM do not end there - CRM will check each order and give a signal as the deadline approaches to help the client not to forget anything.
Keywords: CRM-system, client database, data automation.

УДК 004.05

Мулица Анастасия Витальевна, Хмелевский Сергей Владимирович
Белорусский государственный экономический университет
amulica@mail.ru, sergey-khmelevskiy@mail.ru

Компьютерные преступления как негативная тенденция развития информационной экономики

С момента зарождения общества люди имели потребность общаться друг с другом. Поначалу это происходило в устной форме с помощью жестов и мимики, но с развитием и появлением новых технологий общение также вышло на новый уровень. Появление глобальной сети Интернет и компьютеров привело к тому, что значительная часть информации, как личной, так и коммерческой, стала храниться и передаваться в цифровом формате.

Бесспорно, что большая часть этой информации представлена не в открытой форме, а засекречена, но именно этот факт привел к появлению преступности в данной сфере. Итак, компьютерные преступления - преступления, совершенные в сфере компьютерных и информационных технологий (IT-сфере). Существует более широкое понятие, которое описывает это явление, – киберпреступность [1].

Сегодня во многих странах проводится активная борьба с киберпреступностью. Это может быть обусловлено тем, что в XXI веке информация становится главной ценностью и предметом купли-продажи.

Согласно [2], в Беларуси в 2017 году по сравнению с 2016 уровень киберпреступности вырос на четверть. Количество раскрытых преступлений в сфере высоких технологий в прошлом году по сравнению с тем же 2016 увеличилось с 2471 до 3099. Следует отметить, что 75 % из них – это хищение данных с использованием компьютерной техники.

Так почему же уровень преступности в IT-сфере растет? Неужели так сложно выявить правонарушителей и применить к ним соответствующие санкции?

Ответить на эти вопросы достаточно трудно, так как на уровень раскрытия влияют самые разнообразные факторы.

Если преступление и совершено, то, как правило, сразу факт его совершения заметить почти невозможно. В таких случаях редко наносится вред материальной составляющей компьютера. К примеру, несанкционированное копирование информации чаще остается необнаруженным. Также заражение компьютера вирусами обычно приписывают невнимательности или неосторожности пользователя, который не смог выявить их вовремя. Расследование преступлений такого типа требует специальных знаний и соответствующего программного и аппаратного обеспечения.

Проблема в выявлении подобных правонарушений заключается в том, что потерпевшие чаще всего не стремятся сразу заявлять об этом в правоохранительные органы. А наличие такого факта увеличивает уверенность правонарушителей. Проведя опрос среди студентов нашего потока, мы выяснили, что 75% опрошенных сталкивались с вирусами, полученными вместе с файлами из сети Интернет; 35% заносили вирусы на свои персональные компьютеры с ненадежных съемных носителей; 55% студентов имеют печальный опыт с потерей доступа к аккаунту в социальных сетях, связанного с несанкционированным доступом мошенников к личной странице; 5% опрошенных столкнулись с «логическими бомбами», которые представляют собой несанкционированное внесение набора определенных команд, срабатывающих каждый раз при каких-либо определенных обстоятельствах (они используется только тогда, когда мошенник точно осведомлен, что такие обстоятельства будут созданы) [3].

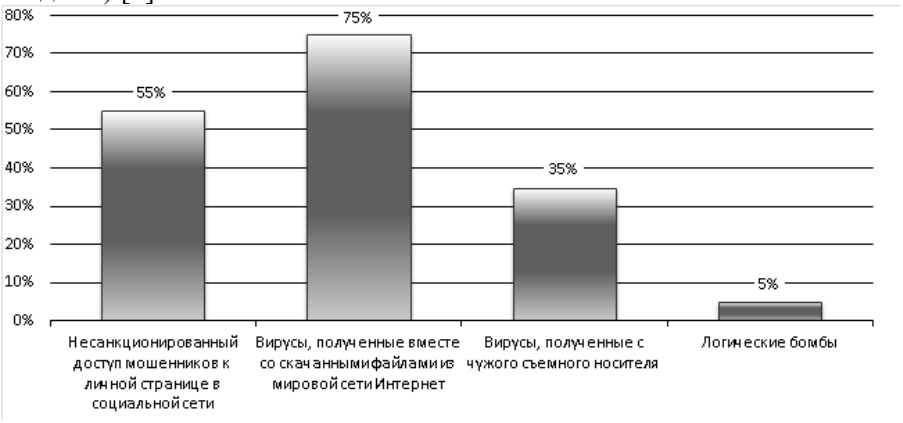

Рисунок 1 - Результаты опроса

Незаинтересованность пострадавших в проведении расследования может быть обусловлена разными причинами. Факт утечки информации, к примеру, может пошатнуть репутацию фирмы. Банковские работники чаще всего стараются скрыть факт кражи информации, поскольку это может вызвать отток клиентов. Некоторые люди не желают раскрывать информацию личного характера или участвовать в затяжном процессе расследования.

В уголовном кодексе Республики Беларусь [4, глава 31] закреплена ответственность за ряд преступлений против информационной безопасности. Так, например, за несанкционированный доступ к компьютерной информации грозит наказание от штрафа до ограничения свободы. Модификация компьютерной информации может повлечь за собой лишение права занимать определенные должности или заниматься определенной деятельностью, арест или ограничение свободы. Компьютерный саботаж – умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя – также относится к преступлению, которое может привести к лишению свободы на срок от 3 до 10 лет. Незаконное завладение компьютерной информацией наказывается общественными работами, или штрафом, или арестом на срок до шести месяцев, или ограничением, или лишением свободы на срок до 2 лет.

Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети – все это наказуемо.

Лица, совершающие компьютерные преступления, чаще всего называют себя «хакерами». Согласно доктору юридических наук, российскому учёному-криминалисту В.Б. Вехову, слово «хакер» во многих случаях обозначает талантливого законопослушного программиста. И чаще всего это оказывается правдой: хакеры - люди, которые стремятся совершить взлом наиболее неординарным способом, «творчески», не стремясь сокрыть содеянное. Однако есть и другая группа взломщиков – кракеры, которые, в свою очередь, бывают 3 видов: вандалы, взломщики и шутники. Последний тип является самым неопасным, и обычно цель таких людей - «факты

немотивированного озорства» [5]. Однако не все мошенники имеют такие безобидные мотивы. Многие из них проводят сложные многоступенчатые финансовые махинации, пытаясь, например, отомстить, наладить шпионаж или даже устроить настоящую диверсию.

Информационное общество и информационная экономика, в частности, на стадии своего становления и развития сталкиваются с разными компьютерными преступлениями, среди которых можно выделить, например, перехват информации (аудиоперехват, видеоперехват, активный перехват (реализуется при физическом доступе к персональному компьютеру), пассивный перехват (реализуемый посредством фиксация электромагнитных излучений), а также «просмотр мусора» (т.е. восстановление и изъятие удаленной или утерянной информации). Следует отметить, что «просмотр мусора» на сегодняшний день как компьютерное преступление в том числе и в экономической сфере является весьма распространенным [6]. В профессиональной среде существуют весьма нетривиальные названия компьютерных преступлений, связанных с перехватом информации [6], например, «за дураком» (незаконный доступ к технике во время отсутствия пользователя на рабочем месте), «неспешный выбор» (если однажды преступнику удастся найти слабое место в защите системы, он многократно может пользоваться им, «не спеша» отбирая нужную информацию), «маскарад» (проникновение в систему путем выдачи себя за законного пользователя), «аварийный» (незаконное использование программного обеспечения, созданного для экстренных сбоев в работе ЭВМ, для обхода систем защиты и контроля), «склад без стен» (использование системной поломки), «подкладывание свиньи» (имитация работы системы), «троянский конь» («троянская матрешка», «троянский червь»), подразумевающий ввод в программное обеспечение вредоносного кода, выполняющего непредусмотренные пользователем действия, «салями» – особая разновидность «троянского коня», основанная на бухгалтерских операциях и активно используемая при совершении финансовых махинаций и другие.

В истории компьютерных преступлений, которая берет начало еще в прошлом веке, одними из наиболее известных нарушителей стали Роберт Морис и Джонатан Джеймс [7]. Роберт Морис является создателем всемирно известного «червя Мориса» в 1988, который

распространялся по сети Интернет. Как говорил сам Морис, он написал этот код «просто из любопытства, чтобы проверить масштабы Всемирной Сети». Но его вирус распространялся настолько активно, что смог стать огромной проблемой для компьютеров по всему миру. После этого Мориса приговорили к 3 годам испытательного срока и штрафу в размере 10 500 долларов США [7].

Джонатан Джеймс прославился тем, что уже в возрасте 16 лет смог взломать подразделение Министерства обороны США. Также на его счету проникновение в сеть NASA. Как говорили журналисты, он украл программное обеспечение на сумму около 1,5 млн. долларов. Хотя сам Джон заявил, что код был слишком легким и столько не стоил [7].

Таким образом, с одной стороны, мировая сеть Интернет, а также развитие информационного общества в совокупности с процессами глобализации сделали информацию более доступной, образование и удаленную работу - проще и реальнее, сблизили людей, дали возможность развиваться информационной экономике и электронному бизнесу. Однако при всех достоинствах, существует и ряд опасных тенденций, в том числе незаконная компьютерная деятельность. Разумеется, новые разработки в области информационной безопасности и совершенствование законодательной сферы позволяют сдерживать интернет-преступников, но ежедневно хакеры находят сотни новых креативных способов обойти закон, дав специалистам по компьютерной безопасности пищу для размышлений. Последние постоянно улучшают физическую защиту помещений, разрабатывают новое программное обеспечение, способствуют ужесточению административных мер, продолжая эту бесконечную гонку, где, кажется, ни одна сторона не может одержать окончательную победу.

Источники литературы

1.История компьютерных преступлений // Компьютерные преступления [Электронный ресурс]. – 27.11.2012. – Режим доступа: https://sites.google.com/site/komputernyeprestuplenia/home/istoria-komputernyh-prestuplenij – Дата доступа: 28.11.2018.

2. «Криминальная» статистика. В Беларуси снижается уровень преступности, но не во всех сферах // TUT.BY [Электронный ресурс]. - 06.03.2018 – Режим доступа: https://news.tut.by/society/583654.html?crnd=88784 – Дата доступа: 28.11.2018.

3.Логическая бомба // ВикипедиЯ [Электронный ресурс]. – 25.01.2016 – Режим доступа: https://ru.wikipedia.org/wiki/ – Дата доступа: 28.11.2018.

4.Законодательство Беларуси о преступлениях в сфере высоких технологий// LAWTREND. Центр правовой трансформации [Электронный ресурс]. – 09.05.2014 – Режим доступа: https://www.lawtrend.org/publications-interview-programmnye-intervyu-

kommentarii-i-publikatsii-ekspertov-prosvetitelskogo-uchrezhdeniya-tsentr-pravovoj-transformatsii/kozluk/aleksej-kozlyuk-zakonodatelstvo-belarusi-o-prestupleniyah-v-sfere-vysokih-tehnologij – Дата доступа: 28.11.2018.
5.Компьютерные преступления // Энциклопедия Кругосвет. Универ-сальная научно-популярная энциклопедия [Электронный ресурс]. – 13.04.2018 – Режим доступа: http://www.krugosvet.ru/enc/ekonomika-i-pravo/kompyuternye-prestupleniya#part-6 – Дата доступа: 28.11.2018.
6.Компьютерные преступления // GRANDARS [Электронный ресурс]. – 02.12.2013 – Режим доступа: http://www.grandars.ru/college/pravovedenie/kompyuternye-prestupleniya.html – Дата доступа: 13.12.2018.
7.Гении компьютерных преступлений // Компьютерные преступления [Электронный ресурс]. – 27.11.2012 – Режим доступа: https://sites.google.com/site/komputernyeprestuplenia/home/primery-komputernyh-prestuplenij - Дата доступа: 28.11.2018.

Mulitsa Anastasiya, Khmelevskiy Sergey
Belarus state economic university

Computer crimes as a negative trend in the development of the information economy

Annotation. The article discusses computer crimes as a negative trend in the development of the information society.

Key words: computer crimes, the Internet, hackers, responsibility.

УДК 633:631.51

Образцов Кирилл Игоревич
Белорусский государственный экономический университет
kirillleopold@gmail.com

Точное земледелие в АПК

В настоящее время сельскохозяйственное производство ежегодно расходует на технологические цели около 1,5 млн тонн автотракторного топлива, 2,7 млрд кВт/ч электроэнергии, 370 млн чел.-ч живого труда. На 1 га пахотных земель в пересчете на условное топливо (у.т.) в Республике Беларусь расходуется 350-400 кг, в то время как, например, в США – 190 кг у.т. В новых экономических условиях увеличение объемов производства сельскохозяйственной продукции, повышение ее качества может обеспечиваться при меньшем удельном потреблении ресурсов. Этим требованиям вполне отвечает инновационная технология точного земледелия.

Точное земледелие — это система управления продуктивностью посевов, основанная на использовании комплекса спутниковых и компьютерных технологий.

Основы точного земледелия были заложены в XX веке. В 1988 году начались первые опыты по использованию новых мобильных агрегатов для смешивания и внесения удобрений. Однако в тот период системы GPS навигации не были настолько точны, как сейчас.