А.Г. Лырчиков,
кандидат биологических наук, доцент Забайкальского государственного университета, доцент

А.Б. Шешуков,
юрисконсульт ОАО «Служба заказчика»

Д.Б. Шешукова,
студентка ЗабГГПУ им Н.Г. Чернышевского

НЕОБХОДИМОСТЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

В статье рассмотрены основные шаги, предпринятые мировым сообществом, для борьбы с кибер-преступностью. Высказаны предложения относительно противодействия данному виду преступления в России.

A.G .Lyurchikov
A.B. Sheshukov
D.B.Sheshukova

THE NECESSITY OF PROVIDING THE SAFETY OF INFORMATIONAL SYSTEMS

In article the basic steps undertaken by the world community for struggle a cyber of criminality are considered. Offers concerning counteraction are stated the given kind of a crime in Russia.

Американский специалист по менеджменту Льюис Д. Эйген заявил: «Скоро останутся лишь две группы работников: те, кто контролирует компьютеры, и те, кого контролируют компьютеры. Постарайтесь попасть в первую».

Переход от индустриального века к информационному – поворотный момент в истории человечества, когда благосостояние и само выживание будущих поколений зависит от уровня защищенности киберпространства (совокупность информационных систем и систем управления, компьютерных и телекоммуникационных сетей, программного обеспечения и технических средств). Сообщения о не санкционированных (пиратских) проникновениях на сайты государственных структур, спецслужб, банков и т.д. в настоящее время появляются довольно часто.

Проанализируем информацию журнала «Шпигель» (август, 2007):

«Как сообщает Der Spiegel, первые следы взлома были обнаружены еще в мае нынешнего года. Киберпреступники, используя заражённые документы в форматах Microsoft Word и PowerPoint, попытались внедрить троянские модули в компьютеры немецких правительственных структур. С тех пор попытки инфицирования не прекращаются. Злоумышленникам удалось внедрить шпионские программы на компьютеры администрации канцлера Ангелы Меркель, а также Министерства иностранных дел, Министерства экономики и Министерства исследований и разработки Германии. Факт незаконного проникновения на компьютеры был установлен специалистами Немецкого федерального бюро информационной безопасности и Федеративного бюро защиты информации. За несколько месяцев немецким

спецслужбам удалось предотвратить утечку 160 Гб данных. Однако – сколько информации смогли похитить злоумышленники, пока не ясно. По версии немецких властей, взлом правительственных компьютеров осуществили китайские хакеры, действовавшие по поручению Народной освободительной армии Китая. При этом шпионские модули распространялись через серверы, расположенные на территории Южной Кореи, что теоретически должно было усложнить обнаружение их первоначального источника…»

Приведем отрывок из письма к Президенту США от лица 50 ученых, компьютерных экспертов и представителей американских разведслужб:

«Рассмотрим следующий сценарий ....

В один прекрасный день террористическая организация заявляет о том, что они отключат Тихоокеанскую Северо-западную электрическую сеть на 6 часов, начиная с 16.00, а затем выполняет обещанное. Эта же группа затем заявляет, что они отключат основную телекоммуникационную магистральную линию связи между Восточным и Западным побережьем США на полдня и выполняет обещанное, несмотря на все наши усилия этому помешать. Затем они угрожают вывести из строя систему управления воздушным трафиком города Нью-Йорк, заставляя приземляться все самолеты и отводя в сторону входящий трафик, и выполняют обещанное. Далее следуют другие угрозы, которые также приводятся в исполнение, демонстрируя возможности наших врагов успешно атаковать нашу критичную сетевую инфраструктуру. Наконец террористы угрожают парализовать сервисы электронной коммерции и кредитных карт на неделю путем использования нескольких сотен тысяч похищенных идентиф по злому умыслу. Все это происходило как изолированные события, распределенные во времени. Некоторые – в результате технических неполадок, другие – были результатом неудачных экспериментов, а некоторые из них – в результате осуществления реальных кибер-атак. Однако все эти события могут быть осуществлены в результате удаленных кибер-атак».

В этом письме, написанном на рубеже XXI века, говорится о проблеме, постепенно выходящей на первый план не только в США, но и в остальном мире, – проблеме обеспечения кибер-безопасности. По инициативе президента США была разработана и опубликована в сентябре 2002 года программа «Национальной стратегии обеспечения безопасности кибер– пространства». Данная стратегия определяет основные принципы, подходы, угрозы, субъекты и объекты защиты и нападения от умышленных и злонамеренных воздействий, а так же способы усиления национальной жизнестойкости компьютерных сетей и технологий. Она включает в себя следующие действия:

1. Введение массовой стандартной защищенной конфигурации операционных систем. Обязательным условием является короткий промежуток времени введения защищенной конфигурации на все компьютеры организации, т.к. это не оставляет времени преступникам на анализ уязвимостей и вмешательство.

2. Создание специальных программ для обнаружения кибер-атак, позволяющих производить непрерывный мониторинг и анализ сетевого трафика, для своевременного обнаружения признаков присутствия в компьютерных сетях не санкционированного проникновения.

3. Усложнение удаленного проникновения в компьютеры при помощи введения двойной идентификации авторизированных пользователей. К паролям добавили карты доступа.

Список литературы

1. *Чеботарева А.А.* Электронное государственное управление как новая форма взаимоотношений личности, общества и государства // Государственная власть и местное самоуправление. 2011. № 6. С. 18-23.
2. *Чеботарева А.А.* Предоставление государственных и муниципальных услуг в электронной форме: реальность 2014 года? // Государственная власть и местное самоуправление. 2010. № 10. С. 16-20.
3. *Чеботарева А.А.* Эволюция института прав человека в условиях развития информационного общества // Государственная власть и местное самоуправление. 2012. № 6. С. 27-33.
4. *Чеботарева А.А.* Актуализация прав и свобод человека в условиях развития электронного государства // Юридический мир. 2011. № 9. С. 48-52.
5. *Чеботарева А.А.* Человек и электронное государство. Право на информационную безопасность. Монография // М-во образования и науки Российской Федерации, Гос. образовательное учреждение высш. проф. образования «Читинский гос. ун-т» (ЧитГУ). Чита, 2011.
6. *Макаров А.В., Чеботарева А.А.* Информатизация деятельности судебных, правоохранительных и иных государственных органов: подходы к реализации и перспективы развития // Арбитражный и гражданский процесс. 2012. № 7. С. 2-5.
7. *Чеботарева А.А., Ермошина Р.А.* Взаимодействие законодательной, исполнительной и судебной власти в реализации информационной функции государства // Российская юстиция. 2010. № 12. С. 56-60.
8. *Чеботарева А.А.* К вопросу о проблемах обеспечения информационной безопасности в таможенных органах // Таможенное дело. 2012. № 2. С. 11-15.
9. *Куняев Н.Н.* Конфиденциальное делопроизводство в системе обеспечения информационной безопасности Российской Федерации // Вестник Академии права и управления. 2012. № 20. С. 5-12.
10. *Белоусов О.Б.* Интеллектуальные программные среды для автоматизированных систем обработки информации // Вестник Академии права и управления. 2010. № 19. С. 87-94
11. *Куняев Н.Н.* Информационная сфера как объект правового регулирования // Вестник Академии права и управления. 2012. № 21. С. 44-49.
12. *Тарасов А.М.* Криптография и электронная цифровая подпись: правовые и организационные аспекты // Вестник Академии права и управления. 2011. № 22. С. 9-19.
13. *Тарасов А.М.* Электронный банкинг и проблемы его безопасности // Вестник Академии права и управления. 2011. № 23. С. 41-51.
14. *Тарасов А.М.* Информационная безопасность в ракурсе международных нормативных актов // Вестник Академии права и управления. 2011. № 24. С. 37-47.
15. *Потапов Н.А.* Законодательный статус конфиденциальной информации в Российской Федерации // Вестник Академии права и управления. 2011. № 24. С. 31– 36.
16. *Чекунов И.Г.* Киберпреступность: проблемы и пути решения // Вестник Академии права и управления. 2012. № 25. С. 97-102.
17. *Чекунов И.Г.* Понятие и типология киберпреступности // Вестник Академии права и управления. 2012. № 26. С. 68-73.
18. *Иванов С.В.* Теоретико-правовой анализ понятия «Информационная – психологическая безопасность личности» // Вестник Академии права и управления. 2012. № 26. С. 130-134.
19. *Тарасов А.М.* Информатизация судебной системы и электронное правосудие // Вестник Академии права и управления. 2009. № 17. С. 5.

20. *Чеботарев, В.Е., Коновалова Е.И.* Использование электронных средств голосования при проведении избирательных кампаний: опыт зарубежных стран и России // Юридический мир. 2012. № 8. С. 44-48.
21. *Чеботарев В.Е., Коновалова Е.И.* Электронное государство, электронное правительство, электронная демократия на современном этапе развития российской федерации // Юридический мир. 2012. № 7. С. 35-38.