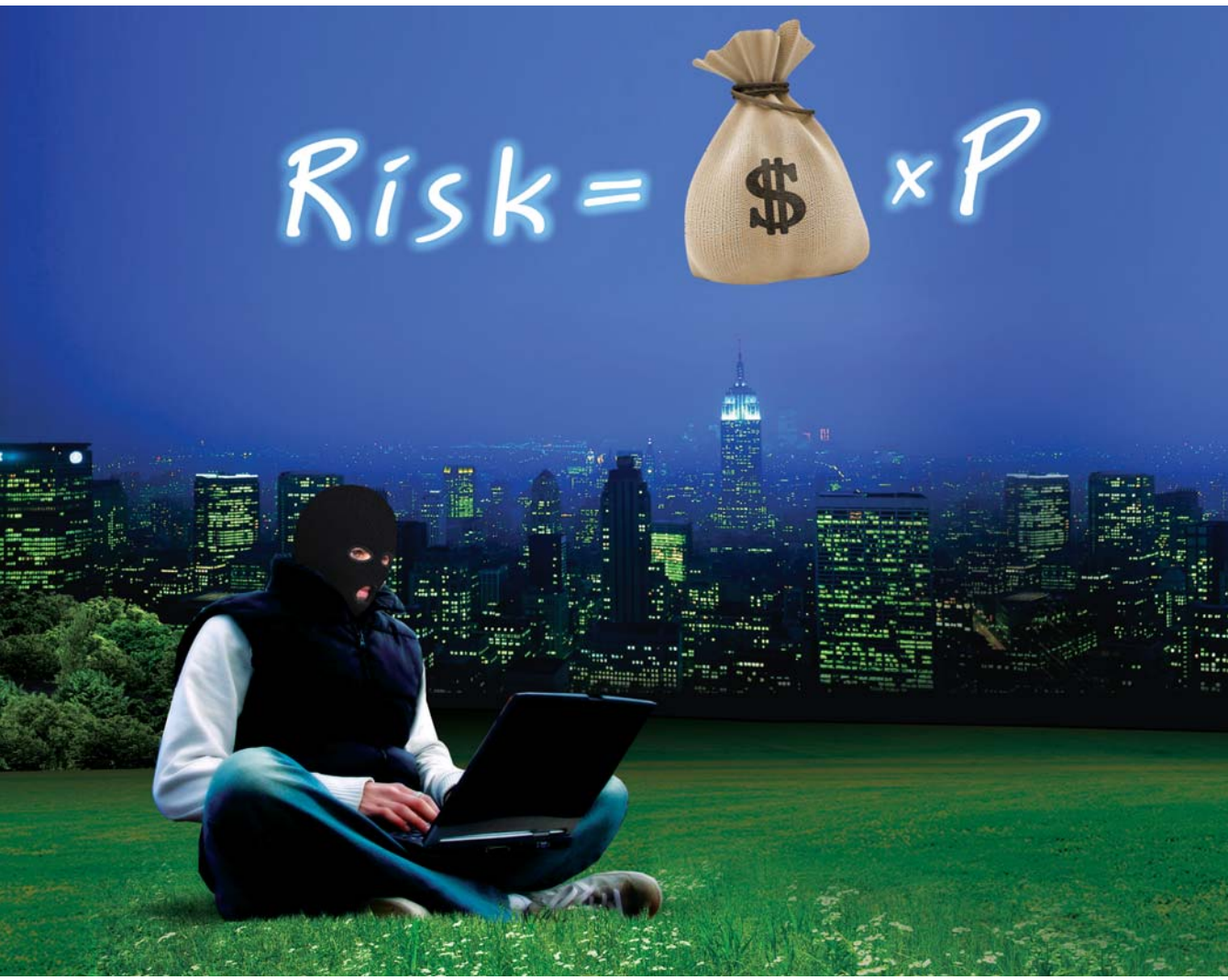
# Искусство управления информационными рисками

*Александр Астахов*




*Настольная книга менеджера информационной безопасности и эксперта по оценке информационных рисков*

Global Trust Solutions

ДМК ИЗДАТЕЛЬСТВО

**УДК 002.6**
**ББК 65.050.2**
**А91**

**Астахов Александр Михайлович**
А91 Искусство управления информационными рисками. — М.: ДМК Пресс, 2010. — 312 с., ил.

**ISBN 978-5-94074-574-7**

В книге подробно излагается системный подход к управлению информационными рисками, основанный на эффективной авторской методологии, многократно проверенной на практике в российских компаниях и полностью совместимой с международными стандартами. Из этой книги вы узнаете:

- как разобраться с информационными активами, угрозами, уязвимостями, механизмами контроля, требованиями безопасности и рисками, а также определить, каким образом все это влияет на бизнес;
- как реализовать на практике риск-ориентированный подход к обеспечению информационной безопасности, построив сбалансированную систему управления рисками;
- как анализировать и оценивать информационные риски бизнеса, успешно справляясь с возникающими при этом трудностями; как оценивать и управлять возвратом инвестиций в информационную безопасность;
- как отличить реальные угрозы от мнимых, а также что такое глобальные информационный кризис и почему он уже не за горами.

Книга ориентирована прежде всего на специалистов по информационной безопасности, ИТ специалистов и риск-менеджеров. Она будет также полезна руководителям компаний, менеджерам всех уровней, имеющим отношение к подготовке и принятию решений по рискам, аудиторам, а также широкому кругу читателей, интересующихся вопросами управления рисками, информационными технологиями и связанными с ними угрозами. Глубина и обстоятельность изложения материала позволяет использовать книгу в качестве учебного пособия для высших учебных заведений и послевузовского образования.

УДК 002.6
ББК 65.050.2



ISBN 978-5-94074-574-7

# СОДЕРЖАНИЕ

ГЛАВА 1

# ПРЕДПОСЫЛКИ ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

*Обязанность ученых — очищать мировоззрение современников от заблуждений.*

Н.К. Кольцов, известный генетик

- Риски, породившие мировой финансовый кризис
- Информационные риски киберпространства
- Обилие стандартов, требований, средств и технологий защиты не уменьшает риски
- Государственное регулирование только создает дополнительные риски
- Оценка рисков как основа корпоративного управления
- Как оценивают риски наши соотечественники

Возможно, для кого-то это и будет новостью, однако анализ ситуации в стране и в мире показывает, что без управления рисками уже невозможно обеспечить стабильность и избежать глобальных кризисов. В этой вступительной главе мы попытаемся осознать важность управления рисками, а также те проблемы, которые решаются путем оценки риска.

Из дальнейшего изложения следует, что уже в наши дни многим организациям управлять рисками совершенно необходимо не только для получения конкурентных преимуществ, но и для выживания. Однако у читателяможет возникнуть резонный вопрос: «Раз это столь важно, тогда каким же образом многие организации до сих пор обходились и обходятся без систематического управления рисками?» На наш взгляд, все дело в том, что времена очень быстро меняются. Раньше управление рисками действительно было не столь актуально из-за незначительного количества информационных угроз, а также ограниченности существовавших тогда технологий и стандартов. Выбирать контрмеры было особенно не из чего, да и защищаться тоже было не от чего.

Сейчас же мир стремительно меняется. Для нового информационного века характерны немыслимые ранее угрозы и кризисы. Количество вредоносных кодов сейчас исчисляется миллионами, а количество известных интернет-

уязвимостей, уязвимостей системного и прикладного ПО — десятками тысяч. Ежедневно регистрируется огромное количество сетевых атак и внутренних инцидентов информационной безопасности. Сложность атак, изощренность способов их реализации и степень опасности возрастает в геометрической прогрессии.

Все это могло бы быть не более чем забавно, если бы столь же стремительно не увеличивалась зависимость критичной для жизнедеятельности людей инфраструктуры и бизнеса от информационных технологий. Взлом очередного веб-сайта может послужить развлекательной новостью и темой для обсуждения в узком кругу посвященных, DDoS-атака (распределенная атака на отказ в обслуживании) против сайтов крупного информационного агентства — это уже новость, получающая более широкий резонанс. Скоординированные атаки на объекты инфраструктуры: электростанции, телекоммуникационные узлы, системы водо-, тепло- и газоснабжения — могут стать причиной глобальной катастрофы, последствия которой даже трудно себе представить.

## Риски, породившие мировой финансовый кризис

*Я занимал пост председателя совета директоров «Росгосстраха», ко мне в 2002 году приезжали немецкие регуляторы и учили, как строить систему контроля в компании, диверсифицировать резервы и т.п. Через полгода вся страховая система Германии рухнула: выяснилось, что две трети компаний — банкроты, так как неправильно считали все риски.*

Рубен Варданян, глава «Тройки-Диалог»

Неправильная оценка рисков является фундаментальной причиной глобальных и локальных кризисов. Без надлежащего управления рисками любая «правильная» система рано или поздно обрушивается. Мы живем сейчас во времена глобального финансового кризиса. Пока точно не известно, с какими потерями наша страна из него выйдет, но уже очевидно — потери эти будут весьма значительными.

Сейчас на первом плане финансовые риски. Однако не так сложно предположить, что в перспективе на смену финансовым кризисам придет кризис информационный, который будет еще опасней.

США «профукали» финансовый кризис из-за того, что не умели (да и не очень хотели) оценивать новые финансовые риски. Обуреваемые жадностью финансисты соорудили самую высокую в истории финансовую пирамиду. Высота этой пирамиды оценивается в десятки квадриллионов несуществующих долларов. Многие специалисты видели эту пирамиду, но, как это обычно бывает, надеялись вовремя «соскочить» до того, как начнется процесс обрушения.

Экс-глава ФРС Алан Гринспен назвал нынешний финансовый кризис самым тяжелым с момента окончания второй мировой войны. По данным американского инвестиционного банка «Голдман Сакс», прямые потери мирового финансового рынка от нынешнего кредитного кризиса составят 1,2 триллиона долларов.

В качестве основной причины нынешнего финансового кризиса эксперты называют: *неправильную оценку рисков* новых производных финансовых инструментов (деривативов) банками, финансовыми институтами, страховыми компаниями и рейтинговыми агентствами.

По мнению экспертов, во всем виновата *секьюритизация* — это способ привлечения финансирования, связанный с выпуском ценных бумаг, обеспеченных активами, генерирующими стабильные денежные потоки, например, портфель ипотечных кредитов, автокредитов, лизинговые активы, коммерческая недвижимость, генерирующая стабильный рентный доход и т.д. В последнее время секьюритизация активов приобретает все большую популярность среди инновационных схем привлечения финансирования и на российском рынке.

Рейтинговые агентства, опираясь на свои безупречные репутации, выпускали рейтинги, как будто *деривативы* — это простые долговые обязательства, выпущенные одним предприятием, но это было неверно. Также были и другие новации, когда первый, начальный пул средств был некредитным, а доходы по траншам были секьюритизованными доходами. В данной ситуации рейтинговые агентства строили более сложную схему рейтингования, но и эти схемы оказались далеки от истины.

В результате осуществления рисков, связанных с деривативами, произошла цепная реакция по всему миру и началась полная переоценка ценностей в финансовом мире. Сейчас никто не верит никаким рейтингам. Все, что считалось надежным вчера, сегодня выглядит крайне рискованным.

Можно с уверенностью утверждать, что подавляющее большинство людей не обладают достаточным объемом информации и квалификацией для того, чтобы предвидеть подобные финансовые кризисы или осознать их причины. Еще значительно меньшее число людей способны осознать возможные причины, механизмы и последствия информационного кризиса, способного в будущем по своим масштабам многократно превзойти нынешний финансовый кризис.

В результате эволюции человечество создало мощнейшую сетевую информационную инфраструктуру на базе открытых стандартов, объединяющую системы связи, обработки информации и управления жизненно важными объектами. После чего начался стремительно набирающий обороты процесс интеграции финансовых, торговых, промышленных систем, систем жизнеобеспечения, средств массовой информации и т.п. в эту единую сетевую инфраструктуру, получившую название *«киберпространство»*.

Киберпростанство — это не только Интернет. Оно объединяет также банковские, частные и ведомственные сети во всех их взаимосвязях. Информационно-техническая революция происходит столь стремительно, что даже специалисты не в состоянии осознать всех рисков, которые несет за собой такая интеграция.

Если бы не новые возможности, предоставляемые киберпространством, нынешний финансовый кризис был бы невозможен. Финансовые рынки одними из первых интегрировались в единое информационное пространство, что позволило миллионам инвесторов свободно и за считанные секунды перемещать любое количество виртуальных активов (денег, ценных бумаг и производных финансовых инструментов) между странами и торговыми площадками. Благодаря современным информационным технологиям стало возможным осуществлять торговлю любыми производными инструментами, что довольно скоро привело к возникновению рынка таких инструментов, образовавших гигантскую финансовую пирамиду, которая рассыпается на наших глазах как карточный домик, погребая под своими обломками экономики целых стран.

Финансовый кризис произошел потому, что никто не знал, как управлять новыми рисками в новых условиях. Благодаря киберпространству возникли новые финансовые риски. В данном случае киберпространство явилось лишь необходимым условием для кризиса. Ситуация может быть еще опасней, когда будут осуществляться риски самого киберпространства. В этом случае пострадают не только финансовые системы, но и все прочие, включая объекты жизнеобеспечения и в ряде случаев военные объекты.

## Информационные риски киберпространства

*Скоро останутся лишь две группы работников: те, кто контролирует компьютеры, и те, кого контролируют компьютеры. Постарайтесь попасть в первую.*

Льюис Д. Эйген,
американский специалист по менеджменту

Риски информационной безопасности, связанные с повсеместной «интернетизацией» и интеграцией информационных систем никто сейчас адекватно не оценивает. Кто-то считает, что жизненно важные системы не имеют Интернет-подключений. Кто-то будет рассказывать сказки про надежный саморегулируемый Интернет. Кто-то будет утверждать, что ущерб от реализации киберугроз не может быть столь масштабным. Кто-то искренне верит в то, что электронные банковские системы, АСУТП или военные системы уж точно надежно защищены. Те же, кому известна реальная картина, почему-то предпочитают помалкивать. А затем вдруг, в один прекрасный день, выясняется, что это все было заблуждением, так как реальных рисков никто не оценивал.

В результате может наступить информационный коллапс. В одночасье могут оказаться заблокированными или выведенными из строя не только финансовые системы, но и системы связи, системы жизнеобеспечения, промышленные предприятия и даже военные объекты. Другими словами — встанет все и сразу. А произойти этот ни с чем не сравнимый кризис, представляющийся сейчас многим не более чем научной фантастикой либо досужими домыслами, может уже в ближайшее десятилетие.

На фоне огромного количества информационных угроз, которым подвержены экономические системы, государства, организации и отдельные граждане, особое место занимают различные формы кибертерроризма, способные нарушить функционирование жизненно важных объектов инфраструктуры, мошеннические операции в системах электронных расчетов и угрозы утечки конфиденциальной информации. Рассмотрим эти классы угроз более подробно, так как каждая из них, а в особенности их объединение, может спровоцировать невиданный доселе мировой информационный кризис.

## Кибертерроризм

*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. Затем они выполняют обещанное. Эта же группа затем заявляет, что они отключат основную телекоммуникационную магистральную линию связи между Восточным и Западным побережьем США на полдня. Затем они выполняют 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, отводя в сторону входящий трафик, и выполняют обещанное. Далее следуют другие угрозы, которые тоже успешно приводятся в исполнение, демонстрируя возможности наших врагов успешно атаковать критичную сетевую инфраструктуру. Наконец террористы угрожают парализовать сервисы электронной коммерции и кредитных карт на неделю путем использования нескольких сотен тысяч похищенных идентификационных номеров в миллионах поддельных транзакций в случае, если их требования не будут удовлетворены. Вообразите, какую панику и всеобщий хаос это вызовет».*

Что делает этот сценарий интересным и волнующим, так это то, что все упомянутые события уже происходили ранее, хотя и не в одно и то же время и не все 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 кибератак. Важен тот факт, что все эти события могут быть осуществлены в результате кибератак.

Цитируемое письмо было написано уже много лет назад, когда кибератаки еще не были столь массовым явлением как сейчас. В наши дни средства массовой информации ежедневно публикуют информацию о десятках и сотнях компьютерных инцидентов, начиная с крупных утечек данных и заканчивая ограблениями банков через Интернет. В России ежегодно совершаются десятки тысяч компьютерных преступлений, а многие «некомпьютерные» преступления также не обходятся без использования компьютеров и реализации информационных угроз. Кибер-преступность ежегодно наносит ущерб государствам и бизнесу по всему миру на миллиарды долларов и имеет тенденцию к значительному росту.

В таком потоке информации недолго утонуть, поэтому позволим себе сделать небольшой экскурс в историю, чтобы читатель смог получить более структурированное представление о ландшафте современных кибер-угроз. Подробная антология кибератак приведена в Приложении № 2.

Официальный отсчет истории кибер-преступности начинается в начале 70-х годов. В 1971 году телефонный фрикер Джон Дрейпер обнаружил, что забавный свист упакованных в коробки зерновых хлопьев (рис. 1) мог быть изменен, для генерации тонального звука с частотой в 2600 герц. Она совпадала с частотой, используемой телефонными компаниями, для указания того, что магистральная линия была доступна для маршрутизации нового запроса. Направление свиста в приемник телефонной трубки разъединяло один конец магистрали, позволяя войти в режим оператора (полезная функция для обслуживающего персонала, а также для фрикеров).

«Проблема состояла в том, что телекоммуникационные компании позволяли таким сигналам попадать в полосу частот линии связи, благодаря чему

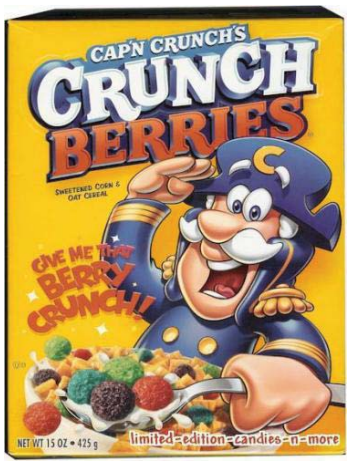



***Рис. 1.*** *Коробка с хлопьями, положившая начало кибер-преступности*

пользователи могли создавать, а также «передавать» эти сигналы. Хотя большинство из этого было перемещено вне полосы передачи сигналов, проблема все еще существует для многих старых коммутаторов, как в некоторых штатах США, так и в ряде мест за границей», — говорит Маддж, хакер, переквалифицировавшийся в компьютерного исследователя в BBN Технологиях. В результате фрикер получает возможность осуществлять бесплатные телефонные звонки и другие противозаконные действия.

Данный эпизод считается прародителем компьютерного хакинга. Дрейпер продолжал создавать «синие коробки», способные к репродуцированию других тонов, используемых телефонной компанией и позволяющих их пользователям делать бесплатные междугородные звонки. Деятельность Дрейпера была освящена в статье журнала «Эсквайр» в 1971 году, которая возбудила интерес творческого дуэта по имени Стив Джобс и Стив Возняк, который самостоятельно начал выпускать «синие коробки». Позднее они основали компанию Apple.

В 1988 году Роберт Т. Моррис, 23-летний студент Корнельского университета, написал некий программный код как часть научно-исследовательской работы, нацеленной на определение размера Интернет. Код предназначался для заражения компьютеров, но только с той целью, чтобы увидеть, сколько существовало подключений в Интернет. Однако, из-за ошибок, допущенных при программировании, все это закончилось использованием уязвимости в ОС Unix и быстрым распространением с многократным заражением множества хостов и выводом их из строя.

Этот случай рассматривается как момент появления первого компьютерного червя, распространяющегося через Интернет, и положившего начало эпохе вредоносного программного обеспечения. Червь Морриса также был первым кибер-инцидентом, получившим заметное внимание со стороны СМИ и судебной системы. В 1990 Моррис был приговорен американским окружным судом к трем годам условного заключения, 400 часам общественных работ и штрафу в размере 10 050 долларов.

В 1995 году начал отбывать свой пятилетний срок Кевин Митник, являющийся волей судьбы, пожалуй, самым знаменитым хакером в истории. В течение двух с половиной лет он взламывал компьютерные системы и крал конфиденциальную информацию у крупных американских корпораций, включая Motorola и Sun Microsystems.

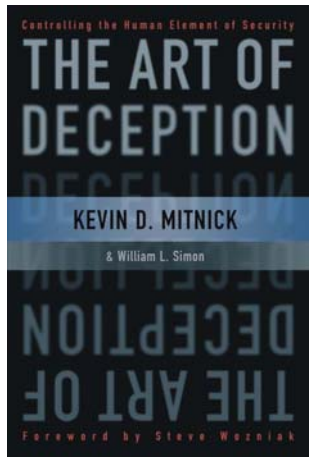



***Рис. 2.*** *Книга Кевина Митника «Искусство взлома»*

Этот случай впервые поместил хакера в центр общественного внимания. Действия Митника наглядно проиллюстрировали концепцию социального инжи-

ниринга — использование манипуляции и обмана вместо технических подходов для получения несанкционированного доступа к компьютерным системам.

Освободившись из мест заключения Кевин Митник встал на путь исправления. Сейчас он руководит собственной компанией и консультирует организации по всему миру по вопросам обеспечения информационной безопасности. Его книга «Искусство взлома» в увлекательной манере повествует о том, каким образом осуществляются атаки и взламываются компьютерные системы.

**2004: Остроумный Червь (Witty Worm)**

Этот компьютерный червь атаковал брандмауэр и другие продукты безопасности компании ISS. Согласно Брюсу Шнеиру, старшему менеджеру по технологиям компании «Бритиш Телеком», после объявления об уязвимости распространение червя пошло очень быстро, заражая 12 000 компьютеров за 45 минут. По сравнению с предыдущими червями этот червь также инфицировал меньшие и более устойчивые к заражению хосты.

*Остроумный Червь* – первое значительное по воздействию вредоносное ПО, использовавшее в своих интересах уязвимость в определенном наборе продуктов безопасности – BlackICE ISS и RealSecure. Это был один из первых червей, которые используют предварительно загруженный список целевых систем. Этот вирус был нацелен на системы обеспечения сетевой безопасности, и ходили слухи, что он был создан сотрудником конкурирующей компании.

**2005: Титановый дождь (Titan Rain)**

Кодовое название, данное правительством США ряду хакерских атак, инициированных из Китая в 2003 году. Целями служили вычислительные сети в Министерстве обороны и других правительственных агентств США.

*Титановый дождь* – первый инцидент кибер-шпионажа национального масштаба. Однако подробности Титанового дождя спорны. Некоторые полагают, что в этом замешано китайское правительство, другие считают, что нападения были работой хакеров, использующих китайские веб-сайты просто для того, чтобы скрыть свои следы.

Наиболее уязвимой в отношении кибератак является инфраструктура самой сети Интернет. Достаточно привести пример сетевого червя Nimda, нанесшего подключенным к Интернет организациям совокупный ущерб, оцениваемый в 3 млрд. долларов.

Некоторые уязвимости Интернет могут приводить к серьезным последствиям и в отсутствии кибератак. Показательным является пример, когда в 1997 году инженер одного из Интернет-провайдеров изменил две строчки кода в конфигурации маршрутизатора, что на три часа привело к останову почты всей глобальной сети. Тем не менее, несмотря на всю серьезность происшедшего, катастрофичным данный инцидент назвать нельзя, хотя совокупный ущерб оказался очень большим за счет того, что урон, хоть и незначительный, был нанесен слишком большому количеству компаний одновременно.

В октябре 2002 года была предпринята беспрецедентная в истории Интернет атака против всей инфраструктуры всемирной сети. Тринадцать корневых DNS-серверов Интернет подверглись распределенной атаке на отказ в обслуживании (DDoS). По словам председателя Консорциума Программного Обеспечения Интернет (Internet Software Consortium Inc.) Пола Викси только четверым из них удалось устоять. Большой уровень избыточности, присущий структуре Интернет, позволил избежать задержек при прохождении трафика, несмотря на выход из строя 2/3 корневых элементов инфраструктуры сети.

Угроза кибертерроризма уже не первый год широко обсуждается в современном обществе на самых разных уровнях, порождая множество споров, мифов и спекуляций. Неадекватная оценка рисков, связанных с осуществлением этой угрозы, приводит как к недооценке, так и к переоценке ее серьезности. В результате, наряду с «устрашающими» описаниями глобальных катастроф, нередко встречается и полное игнорирование этой проблемы. Понятие кибертерроризма часто используется для политических спекуляций и «запудривания мозгов» непосвященным.

Подключение к сети Интернет открывает дополнительные возможности проникновения злоумышленников в компьютерные системы, однако сам факт наличия такого подключения не следует во всех случаях рассматривать как уязвимость. Серьезные меры по резервированию данных и оборудования, предпринимаемые предприятиями различных отраслей, в большинстве случаев обеспечивают адекватный уровень защищенности, даже при успешном осуществлении кибератаки.

К таким выводам автор пришел в 2003 году, когда писал статью под названием «Реалии и мифы кибертерроризма». За прошедшие шесть лет риски киберпространства существенно возросли. Возможно, в ближайшем будущем нашу оценку этих рисков придется пересмотреть в большую сторону.

## Риски промышленных систем

Автоматизированные системы управления (АСУ и АСУТП) в настоящее время используются в большинстве отраслей промышленности, в нефте- и газодобыче, на электростанциях и железных дорогах, на пивоварнях и лыжных

курортах. В мире эксплуатируются миллионы промышленных систем, стоимость каждой из которых измеряется десятками тысяч и миллионами долларов. Степень зависимости критической инфраструктуры государства от таких систем неуклонно возрастает, и вопросы обеспечения их информационной безопасности приобретают первостепенное значение.

В отличие от других видов автоматизированных информационных систем, промышленные системы, особенно те, которые используются для управления критической инфраструктурой, имеют ряд особенностей, обусловленных их особым назначением, условиями эксплуатации, спецификой обрабатываемой в них информации и требованиями, предъявляемыми к функционированию. Главной же особенностью этих систем является то, что с их помощью в автоматическом, либо полуавтоматическом, режиме в реальном времени осуществляется управление физическими процессами и системами, от которых непосредственным образом зависит наша безопасность и жизнедеятельность: электричество, связь, транспорт, финансы, системы жизнеобеспечения, атомное и химическое производство и т.п.

Промышленные системы эволюционировали от экзотических программных и аппаратных средств в 70-х годах прошлого века до вполне современных систем, в которых используются стандартные IBM-совместимые ПК, операционные системы семейства Microsoft Windows, сетевые протоколы TCP/IP, Web-браузеры и Интернет-подключения. Благодаря такой стандартизации, а также распространенной практике подключения промышленных систем к локальным сетям (ЛВС) предприятий и использованию в них технологий беспроводного доступа, множество угроз в отношении этих систем значительно расширилось.

Угрозы в отношении промышленных систем, в зависимости от того, кто выступает в качестве «агента угрозы», можно разделить на следующие основные группы:

1. *Вредоносное ПО.* Промышленные системы, так же как и любые другие ИТ системы, потенциально подвержены угрозам со стороны компьютерных вирусов, сетевых червей, троянских программ и программ шпионов.
2. *Инсайдеры.* Недовольные внутренние пользователи, хорошо знающие систему изнутри, как показывает практика, представляют собой одну из основных угроз. Инсайдер может умышленно повредить оборудование или программное обеспечение. Администраторы и инженеры, обслуживающие систему, могут также неумышленно нанести вред ее функционированию, допустив ошибку в настройках системы или нарушение определенных правил безопасности.
3. *Хакеры.* Аутсайдеры могут быть заинтересованы в исследовании возможности получения доступа и контроля над системой, мониторинге трафика и реализации атак на отказ в обслуживании.

4. *Террористы.* Это наиболее серьезная угроза, создающая основные различия между системами, относящимися к критической инфраструктуре и обычными ИТ системами. Террористы заинтересованы в том, чтобы вывести систему из строя, нарушить процессы мониторинга и управления либо получить контроль над системой и нанести как можно больший вред.

---

В Афганистане были получены доказательства того, что террористическая организация Аль Кайда проявляет повышенный интерес к промышленным системам. Можно также предположить, что среди членов Аль Кайды имеются квалифицированные специалисты (например, арестованный Халид Шейх Мухамед, их главный распорядитель, обучался на инженера в Северной Каролине, а позже работал в водной промышленности на Среднем Востоке).

По сообщению газеты Вашингтон Пост в Афганистане был найден ноутбук, принадлежащий людям Аль Кайды. Было установлено, что с этого ноутбука многократно посещался французский Интернет-сайт, принадлежащий некому Анонимному Обществу (Societe Anonyme). На этом сайте размещено «Руководство по саботажу», содержащее такие разделы, как «планирование нападения», «методы ухода от наблюдения» и т.п. Имеются также свидетельства, подтверждающие, что с компьютеров, принадлежащих террористам, осуществлялся поиск в Интернет программных средств для взлома сетей.

Следователи из США зафиксировали посещения людьми из Аль Кайды сайтов, предоставляющих ПО и инструкции по программированию цифровых переключателей, используемых в энергетических, водных, транспортных и коммуникационных сетях. На некоторых допросах, люди Аль Кайды в общих словах выражали намерения использовать эти инструменты.

Еще совсем недавно в качестве основных источников угроз для безопасности киберпространства США рассматривались Китай, Россия и другие страны. Считалось, что люди Аль Кайды «менее квалифицированы в области использования сетевых технологий», чем многие рядовые хакеры, и поэтому не представляют здесь серьезной угрозы. В связи с указанными фактами разведслужбы США изменили свое мнение относительно возможности использования киберпространства террористами.

---

К счастью, в критичных отраслях, преимущественно использующих промышленные системы, отсутствуют два основных мотивирующих фактора для киберпреступности. Это экономические стимулы, к которым относятся кредитные карты и электронные счета, лежащие в основе многих компьютерных преступлений, и коммерческие тайны, являющиеся основной целью промышленного шпионажа.

Существует большое количество зарегистрированных инцидентов безопасности, затрагивающих системы управления критической инфраструктурой. В ряде научно-исследовательских институтов, ФБР и других организациях ведется соответствующая статистика. Согласно этой статистике в США на промышленные системы осуществляется не менее 100 кибератак в год и существует тенденция к непрерывному увеличению их числа. Зафиксированы все категории кибератак, за исключением кибертерроризма.

Справедливости ради следует признать, что, хотя теоретически и существует возможность электронных вторжений в критичные системы управления, создающих серьезные, в том числе и физические, угрозы безопасности, получение контроля над такими системами извне является крайне маловероятным событием. В настоящее время реальность такова, что было бы проще и дешевле разбомбить цель, чем поразить ее путем взлома компьютерной системы.

Кибератаки действительно могут иметь серьезные последствия, хотя и не связанные с нанесением ущерба жизни и здоровью людей, массовыми разрушениями и другими катастрофами. В худшем случае, хорошо спланированная массированная кибератака может временно вывести из строя системы телекоммуникаций в густонаселенных районах. (Описание наихудших возможных сценариев кибер-атак приведено в Приложении №3).

---

Ядерный завод в штате Агайо функционировал в автономном режиме в течение года после того, как сетевой червь SQL Slammer привел к отключению Системы Отображения Периметра Безопасности на пять часов и заводского компьютера, используемого для мониторинга производственного процесса, на шесть часов. Для обеих систем были предусмотрены дублирующие аналоговые системы, которые не пострадали. Заводская производственная сеть была непосредственно подключена к корпоративной сети, в которую «червь» проник по удаленному каналу из партнерской сети.

Примером хакерской атаки на критическую инфраструктуру США может служить удаленный взлом в 2001 году компьютерной сети Независимого Системного Оператора Калифорнии, управляющего электросетью штата. Хотя тогда хакерам не удалось получить доступ к действующей системе управления электросетью, они имели доступ к корпоративной сети в течение 17 дней. Намерения хакеров и их происхождение так и остались невыясненными.

---

На начальном этапе развития в промышленных системах использовалось малоизвестное специализированное оборудование и программное обеспечение, а их сетевое взаимодействие с внешним миром было сильно ограничено.