УДК 007:35 + 005.5

ПОДХОД К КЛАССИФИКАЦИИ КИБЕРНЕТИЧЕСКИХ УГРОЗ

Ю.Г. Даник, В.И. Шестаков, С.В. Чернышук

Большинство современных исследователей рассматривают кибернетические угрозы гражданину, обществу, государству с точки зрения обеспечения информационной безопасности или защиты информации и не учитывают особенности процессов управления, протекающих в информационных системах. Целью данной работы является развитие подходов к классификации КУ с учетом особенностей процессов управления. Предложено рассматривать кибернетические угрозы как угрозы процессам управления на разных уровнях. Исходя из этого существующие классификации кибернетических угроз дополнены наиболее существенными признаками с точки зрения защиты и противодействия, а также продемонстрирована возможность практического применения предложенной классификационной схемы в отношении информационно-управляющих систем. Полученные результаты позволяют систематизировать накопленные в данной предметной отрасли знания и в дальнейшем использовать их при разработке моделей кибернетических угроз, способов их обнаружения и мероприятий противодействия в интересах обеспечения кибернетической безопасности гражданина, общества, государства.

Ключевые слова: кибернетическая безопасность, кибернетическая угроза, классификация.

Введение

В нормативных документах по вопросам обороны и безопасности ведущих государств мира главное место отводится проблеме противодействия кибернетическим угрозам (КУ). В частности в [1, 2], КУ отнесены к актуальным угрозам национальной безопасности государства, а создание системы кибернетической безопасности (КБ) и защита от кибернетических атак определены как неотложные задачи, требующие незамедлительного решения.

Обеспечение КБ граждан, общества, государства требует, в первую очередь, заблаговременного обнаружения КУ объекту защиты для прогнозирования возможных последствий проявления таких угроз и своевременного принятия решения об их нейтрализации или сдерживании [3, 4]. При условии успешного выполнения указанных действий достигается такое состояние защищенности кибернетического пространства государства от любого деструктивного влияния, при котором обеспечивается его надлежащее функционирование и устойчивое развитие.

Обнаружение КУ требует глубокого анализа их сущности и систематизации таких угроз. Упорядочивание всего множества КУ по определенным классификационным признакам позволит обеспечить необходимый уровень достоверности их идентификации. Поэтому задача классификации существующих и потенциальных КУ объекту защиты является актуальной с точки зрения обеспечения его КБ.

Анализ доступных авторам работ позволяет утверждать, что известные подходы к классификации КУ ориентированы на несколько суженное понимание КУ. В большинстве таких классификаций рассматриваются информационные угрозы [5], угрозы информации [6], угрозы распределенным системам обработки данных [7], то есть угрозы, ориентированные на информационную составляющую безопасности, а не на кибернетическую в целом [8].

При этом авторами указанных трудов в качестве классификационных признаков выбраны такие характеристики угроз, которые присущи узкоспециализированным отраслям деятельности. Например, в [4] речь идет об угрозах специальным информационно-телекоммуникационным системам, в [5] внимание акцентируется на информационно-психологических угрозах, в [6] рассматриваются угрозы в сети Интернет, в [7] систематизированы угрозы, которые возникают в процессе обработки персональных данных, в [9] описаны угрозы в сфере защиты прав интеллектуальной собственности и т. п. Такие подходы характеризуют разные аспекты безопасности процессов управления и обмена информацией, протекающих в подавляющем большинстве систем разных отраслей жизнедеятельности современного общества. В соответствии с современными представлениями подобные системы принадлежат к классу кибернетических.

Таким образом, известные классификации КУ разработаны с позиций обеспечения информационной безопасности и безопасности информации, не учитывают особенности процессов управления, протекающих в кибернетических системах (КС) различного назначения.

Предметом данного исследования является КУ в их широком понимании, целью статьи – развитие подходов к классификации КУ с учетом особенностей процессов управления для систематизации накопленных в данной предметной отрасли знаний и их дальнейшего использования при разработке моделей таких угроз, способов их обнаружения и мероприятий противодействия в интересах обеспечения КБ гражданина, общества, государства.

Классификационная схема кибернетических угроз

По результатам анализа, приведенного в [10], под КУ предлагается понимать факторы (события, явления) информационного, коммуникационного, компьютерно-сетевого, социального и социотехнического пространств (или их комбинацию в определенном сочетании), которые при условии их преднамеренного целенаправленного использования создают опасность нарушения процессов управления, обработки и передачи информации, протекающих в КС различных сфер (социальной, технической, социотехнической), или могут нанести ущерб элементам таких систем.

Исходя из того, что любая классификация является разделением предметов разного рода на взаимосвязанные классы в соответствии с наиболее существенными признаками, свойственными предметам этого рода и отличают их от предметов других родов, к ней выдвигаются следующие требования:

– полнота разделения: все категории классификации должны быть перечислены;

– чистота: категории классификации не должны пересекаться.

Соответственно решение задачи классификации КУ предусматривает формирование как можно более полного перечня таких угроз и распределение их по наиболее существенным и важным в практическом отношении признакам, не допускающим дублирования.

Исходя из сущности КУ при формировании наиболее полного их перечня целесообразно учитывать:

– характеристику конкретной КС и ее элементов;

– особенности процессов управления, обработки и обмена информацией, протекающих в КС;

– свойства среды (путей) распространения сигналов и передачи информации;

– возможности источников (субъектов) угрозы.

К характеристикам КС, которые определяют уровень опасности ее функционированию, можно отнести: структуру КС (элементы системы и взаимосвязи между ними), наличие связей с внешней средой и другими КС, наличие подсистемы защиты.

В общем случае КС состоит из объекта управления, субъекта управления и каналов связи (рис. 1), где $\vec{g}_i'(t)$, $\vec{g}_i''(t)$ – кибернетические угрозы; $\vec{x}(t)$ – входное (управляющая) действие; $\vec{y}(t)$ – реакция системы; t – время. Природа всей системы определяется ее назначением и, обычно, является комбинированной, при этом природа отдельных элементов может быть абсолютно разной: биологической, технической или социальной.

Особенности процессов управления, обработки, и передачи информации, протекающих в КС, обусловлены спецификой алгоритмов превращения входного действия $\vec{x}(t)$, которое поступает через рецепторы, в результат на выходе КС (см. рис. 1). Нарушение любого из этапов данных алгоритмов в результате реализации угрозы $\vec{g}_i(t)$ может привести к дезорганизации функционирования КС и невыполнению ее назначения. Поэтому при рассмотрении каждой конкретной КС важно четко определить участников процесса управления; множество их допустимых состояний и законы изменения таких состояний; сигналы, которые они могут генерировать; безопасные связи между участниками процесса управления.

Каналы связи, представляющие среду передачи информации (управляющих сигналов), являются одним из наиболее уязвимых элементов КС, поскольку во время передачи информации она может перехватываться, модифицироваться или вообще уничтожаться.

Возможности источников (субъектов) КУ обусловлены совокупностью способов доступа (проникновения, влияния) к элементам КС, в результате реализации которых достигается нарушение функционирования таких элементов или выведения их из работоспособного состояния.

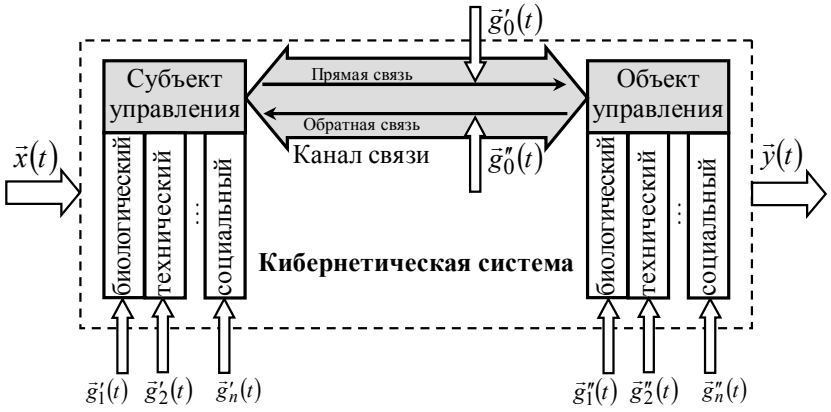

Рис. 1. Модель кибернетической системы

Учитывая особенности функционирования КС, к базовым признакам классификации предлагается отнести следующие (рис. 2):

– вид КС (*V*), на которую направлена угроза;
– элемент КС (*K*), на который непосредственно нацелена реализация угрозы;
– уязвимости (*U*) (системы и ее элементов), которые используются;
– расположение источника (субъекта) КУ (*S*);
– способ реализации КУ (*R*);
– среда распространения (*M*);
– умышленность (*B*);
– происхождение (*N*);
– повторяемость появления (*F*);
скрытность проявления (*L*);
– масштабы последствий от реализации угрозы (*I*);
– иерархия управления, осуществляемого в КС (*Q*);
– целесообразность реализации КУ (*X*);
– время появления КУ (*T*);
– условность реализации (*Y*).

По виду КС (ее физической природе), на которую направлена КУ, различают: технические (V_1); биологические (V_2); социальные (V_3); комбинированные (V_4).

Следует отметить, что вид подлежащей защите КС ограничивает не только диапазон ее потенциальных угроз, но и в значительной степени возможные мероприятия противодействия таким угрозам. Так, например, при рассмотрении сугубо технических КС, можно отбросить угрозы биологической или социальной природы, что позволит сократить перечень возможных мероприятий защиты и противодействия.

По элементу КС (*K*), на который непосредственно нацелена (или через который осуществляется) КУ, можно выделить следующие классы угроз: угрозы объекту управления (K_1); угрозы субъекту управления (K_2); угрозы каналу связи (передаваемой информации, командам) (K_3); комплексные угрозы (K_4).

Классификация по такому признаку, как элемент КС, на который направлена угроза, позволяет повысить эффективность противодействия за счет рационального использования сил и средств (ресурсов) защиты. Заблаговременное сосредоточение ресурсов защиты на определенной составляющей КС, относительно которой существует угроза, позволяет обеспечить необходимый уровень защиты всей системы с наименьшими расходами.

По уязвимостям (*U*) *(*системы и ее элементов), которые используются, имеют место следующие угрозы: угрозы, которые реализуются за счет уязвимостей, свойственных составляющим КС (U_1); угрозы, которые реализуются за счет использования уязвимостей подсистемы защиты КС (U_2); угрозы, которые реализуются за счет недостатков в алгоритмах управления и обработки информации (сигналов) (U_3).

Классификация угроз по используемым уязвимостям позволяет повысить точность локализации опасности и тем самым минимизировать расходы на защиту КС.

Рис. 2. Классификационная схема кибернетических угроз

По расположению (S) источника (субъекта) КУ относительно объекта, на который она направлена, следует выделять угрозы: внешние (S_1) и внутренние (S_2).

Объекты, с которыми взаимодействуют подлежащие защите КС, выступают в качестве источника внешних угроз, а составляющие таких систем – внутренних.

Внешние КУ, в свою очередь, разделяются на угрозы от среды функционирования КС и угрозы от конкурирующих (противодействующих) систем. К угрозам первого подкласса можно отнести стихийные бедствия, революции и т. п. Примером угроз второго подкласса могут быть угрозы противоборствующих сторон друг другу в военном конфликте.

Класс внутренних КУ разделяется с учетом состава конкретной КС. Например, к внутренним КУ современных информационно-управляющих систем можно отнести угрозы от носителей информации; технических средств; программных средств; средств защиты информации (аппаратных, алгоритмических, программных); человека-оператора (обслуживающего персонала) и т. п.

Заблаговременное определение источника угрозы позволяет применять относительно него активные (превентивные) мероприятия противодействия.

Способ реализации КУ (R) зависит от конкретного объекта и его особенностей (технических, социальных, биологических, психологических), но в общем случае выделяются: угрозы, которые предусматривают активное вмешательство в процесс функционирования КС (активные КУ) (R_1); угрозы, которые непосредственно не воздействуют на работу КС (пассивные КУ) (R_2); угрозы с комплексным характером воздействия (R_3).

По среде распространения угрозы (M) выделяются классы, отвечающие существующим опасным средам: информационной (M_1); коммуникационной (M_2); компьютерно-сетевой (M_3); социотехнической (M_4).

Среда распространения КУ в значительной мере определяет формы и способы противодействия таким угрозам. Например, нецелесообразно (хотя и возможно) применять физическое уничтожение коммуникационных каналов для защиты от атаки типа «отказ в обслуживании», а вот нанесение превентивного удара по противнику, который готовится к вооруженной агрессии, можно считать эффективным.

По умышленности (B) угрозы бывают: умышленными (B_1); неумышленными (B_2).

Умышленные угрозы предусматривают осознанное намерение причинить вред КС или ее элементам. Неумышленные угрозы возникают и реализуются безотносительно к воле носителя (источника) угрозы.

По происхождению (N) можно выделить угрозы: искусственного происхождения (антропогенные, техногенные) (N_1); естественного происхождения (N_2).

Угрозы искусственного происхождения являются следствием деятельности человека или функционирования технических систем. Угрозы же естественного происхождения возникают в результате естественных процессов, происходящих в живой и неживой природе.

По повторяемости появления (F) выделяются угрозы: повторяемые (периодические, апериодические) (F_1); неповторяемые (F_2).

Отнесение той или иной угрозы к классу повторяемых позволяет эффективнее противодействовать ей в будущем за счет формирования образа такой угрозы и применения отработанного алгоритма противодействия. Неповторяемые же угрозы требуют привлечения более значительных ресурсов для их устранения в силу необходимости дополнительного изучения и моделирования. Показатель повторяемости f может быть определен, к примеру, количеством m случаев появления той или иной КУ в некотором временном интервале t ($f = \frac{m}{t}$).

По скрытности проявления (L) выделяются: скрытые (L_1); не скрытые (L_2).

Уровень скрытности угроз определяет сложность алгоритмов их идентификации, которая непременно отражается на длительности обнаружения угроз и в конечном итоге определяет принципиальную возможность такого обнаружения за допустимое время.

Скрытность КУ может быть оценена вероятностью обнаружения ее признаков:

$$P_{\text{обн}} = \prod_{j=1}^{N}\left(1 - \prod_{q=1}^{K}\left(1 - P_{\text{обн}_q}\right)\right), \tag{1}$$

где $P_{\text{обн}_q} = \frac{m_{\text{обн}}}{Nl}$ – вероятность обнаружения q-го этапа реализации КУ ($m_{\text{обн}}$ – количество случаев обнаружения q-го этапа, l – количество итераций q-го этапа КУ в каждой из N попыток ее реализации); K – количество этапов реализации КУ.

Реализация любой из КУ или их совокупности может привести к последствиям *разного масштаба* (O) для КС или ее элементов. Соответственно и КУ можно разделить на: локальные (O_1); частично системные (O_2); общесистемные (O_3).

Локальные угрозы характеризуются несущественным осложнением работы отдельного элемента КС, не отражающимся на функционировании КС в целом.

Угрозы частично системного характера приводят к нарушению работы нескольких элементов или сегмента КС, которое может негативно отразиться на выполнении КС части своих функции или назначения в целом с возможностью возобновления пораженного сегмента.

Общесистемные угрозы нацелены на поражение нескольких сегментов системы или ее ключевых элементов, что непременно приводит к отказу функционирования КС в целом без возможности возобновления ее работы.

Степень тяжести последствий реализации угрозы может быть оценена выражением

$$O = \sum_{w=1}^{E} \alpha_w P_w, \tag{2}$$

где α_w – коэффициент важности w-го элемента (сегмента) КС для функционирования системы в целом; P_w – вероятность реализации КУ, нацеленной на w-й элемент (сегмент) КС; E – количество элементов (сегментов) КС.

По иерархии управления (Q), осуществляемого в КС, выделяются КУ: высшего (стратегического) уровня (Q_1); среднего (оперативного) уровня (Q_2); низшего (тактического) уровня (Q_3).

На высшем (стратегическом) уровне управления принимаются и реализуются наиболее важные решения для КС в целом. Очевидно, что угрозы этого уровня наиболее опасны для функционирования КС.

Промежуточный (оперативный) уровень обеспечивает управление ходом отдельных операций (оперативное управление), поэтому является не просто буфером между высшим и более низким звеньями управления, а играет крайне важную роль в исполнении КС своего назначения. Нарушение управления в промежуточном звене может привести к дезорганизации КС, поэтому угрозы на промежуточном уровне управления также представляют опасность.

Низшее (тактическое) звено управления, как правило, является наиболее многочисленным (что позволяет применять в управлении дублирование и резервирование), поэтому угрозы на этом уровне не представляют значительной опасности, а могут лишь повлиять на реализацию определенной частичной функции КС. Однако одновременная реализация некоторой совокупности КУ относительно критических элементов на низшем уровне управления может привести к синергетическому эффекту, потому безопасностью этого звена управления КС также не следует пренебрегать.

Принятие решения о целесообразности (X) реализации КУ возможно по критерию «эффективность/стоимость» ($X = P/C$). То есть, если полученный от реализации КУ эффект P превышает расходы C на ее подготовку и осуществление ($X > 1$), есть смысл рассматривать возможность такой угрозы. В противном случае ($X \le 1$) реализация КУ нецелесообразна. В соответствии с этим выделим такие классы КУ: гипотетически возможные, но маловероятные (X_1); с высокой вероятностью реализации (X_2).

Важным фактором, который влияет на вероятность реализации той или иной КУ, является ее зависимость от определенных событий. То есть, реализация одних КУ возможна лишь при условии, что состоится соответствующее благоприятное событие ω_s (или группа событий $\Omega = \{\omega_1, \omega_2, \ldots, \omega_p\}$), а реализация других – не требует выполнения такого условия.

Соответственно *по условности реализации* (Y) выделим КУ: условные (Y_1); безусловные (Y_2).

Математически безусловные КУ описываются выражением

$$P(A \mid \omega_s) = P(A), \tag{3}$$

а условные:

$$P(A) = \sum_{i=1}^{p} P(\omega_s) P(A \mid \omega_s), \tag{4}$$

$$P(A) = \prod_{i=1}^{p} P(A \mid \omega_s), \tag{5}$$

где A – реализация КУ; ω_s – благоприятное для реализации КУ событие, $\sum_{s=1}^{p} P(\omega_s) = 1$; p – количество благоприятных для реализации КУ событий.

При этом если события ω_s составляют полную группу событий Ω, применяется формула (4), в противном случае – формула (5).

По времени появления КУ (T) выделим: угрозы, которые заложены при создании КС (T_1); угрозы, которые возникают в процессе функционирования КС (T_2).

Несовершенство структуры и конструкции КС или ее отдельных элементов порождают уязвимые места, которые потенциально могут использоваться для нарушения устойчивой работы системы. Такие уязвимости закладываются во время создания системы или проявляются в процессе ее функционирования (для компьютерных систем это «угрозы нулевого дня»). Обнаружение заложенных при создании КС уязвимостей позволяет значительно повысить защиту таких систем от КУ уже на ранних этапах эксплуатации. Уязвимости, которые проявляются со временем, более опасные, поскольку их возникновение сложно предусмотреть или спрогнозировать, поэтому противодействие угрозам, которые используют такие уязвимости, очень затруднено.

Примененный для классификации КУ признаковый принцип позволяет описать любую угрозу $\vec{g}_i$ множеством качественных и количественных признаков $\vec{g}_i = (V, E, U, S, R, M, B, N, F, L, O, Q, X, Y)$, которые могут быть использованы при моделировании и дальнейшей идентификации такой угрозы.

Приведенная классификация КУ предусматривает возможность дополнения и разветвления на подклассы, что достаточно удобно при разработке перечня угроз для каждой конкретной КС, в зависимости от уровня необходимой детализации.

Рассмотрим, к примеру, некоторую КС, принадлежащую к классу информационно-управляющих систем, которые на данное время получили наибольшее распространение. Такие системы состоят из информационных и программно-аппаратных элементов, а также операторов, которые их эксплуатируют.

Основными элементами такого класса КС являются:

– массивы данных как совокупность информации и ее носителей;

– технические средства, автоматизирующие процессы, которые происходят в системе (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации и команд, другие исполнительные технические средства, средства и система охранной и пожарной сигнализации, средства и система оповещения, контрольно-измерительная аппаратура, средства кондиционирования, электроснабжения, связи, оргтехника и т. п.);

– программные средства (операционные системы, системы управления базами данных и т. п.);

– средства защиты информации (аппаратные, алгоритмические, программные);

– человек-оператор (обслуживающий персонал) со всеми присущими психофизиологическими состояниями и реакциями.

Учитывая характер информации, обеспечивающей функционирование информационно-управляющей системы, предложенную классификацию можно расширить, и в классе угроз канала связи (передаваемой информации, командам) выделить подклассы: по виду передаваемой информации; по виду нарушаемого свойства информации; по цели реализации угрозы и т. п.

Принимая во внимание наличие в контуре управления информационно-управляющей системы операторов, можно выделить следующие способы реализации КУ: информационно-психологическое влияние; психогенное влияние; психоаналитическое влияние; нейролингвистическое влияние; психотронное влияние; психотропное влияние.

Рассматривая особенности процессов управления и обмена информацией, протекающих в таких системах, следует отметить, что на данный момент они осуществляются согласно эталонной модели взаимодействия открытых систем ISO/OSI, изложенной в стандарте ISO 7498. КУ как фактор, который влияет на процессы управления и передачи информации, может быть спроектирован на эталонную модель. Поэтому класс КУ, характерный открытым системам, можно расширить такими подклассами угроз: физического уровня; канального уровня; сетевого уровня; транспортного уровня; сеансового уровня; уровня представления; прикладного уровня.

Выводы

Комплексная природа КУ требует рассматривать их, в первую очередь, как угрозы процессам управления, протекающим в КС, а не только информации, циркулирующей в таких системах. Значительное разнообразие КС (по природе, структуре, принципам и среде функционирования и т. п.) обусловливает следующие требования к классификационным признакам КУ: адекватность для любых КС; универсальность, с учетом особенностей процессов управления, обработки и обмена информацией, протекающих в КС разных классов; отражение свойств среды функционирования КС; учет возможностей источников (субъектов) угрозы.

Предложенная классификация КУ не противоречит известным и учитывает при этом комплексный характер таких угроз. В ее основу положены наиболее значимые для обнаружения и противодействия КУ признаки, которые одновременно обеспечивают полноту и чистоту классификации. Приведенные признаки целесообразно использовать для их дальнейшей формализации, а также разработки моделей угроз. Предложенная классификация может послужить основой для разработки методик обнаружения КУ, позволяющих своевременно реагировать на такие угрозы и предотвращать их эскалацию.

По мере постоянного видоизменения современных КС и протекающих в них процессов актуальность классификации КУ можно обеспечить только путем ее постоянного дополнения и уточнения.

Литература

1. National Cyber Security Strategies in the World. – http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (дата обращения: 09.01.2014).

2. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. – http://www.scrf.gov.ru/documents/6/113.html (дата обращения: 05.08.2013).

3. Корнюшин, П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2003. – 154 с.

4. Бурячок, В.Л. Завдання, форми та способи ведення воєн у кібернетичному просторі / В.Л. Бурячок, Г.М. Гулак, В.О. Хорошко // Наука і оборона. – 2011. – № 3. – С. 35–42.

5. Інформаційна безпека держави: аспект інформаційно-психологічних загроз / В.Г. Головань, О.М. Дроздов, В.В. Сергєєв, В.М. Герасимов // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. – 2011. – Вип. 5. – С. 33–41.

6. Конев, А.А. Подход к построению модели угроз защищаемой информации / А.А. Конев // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 34–40.

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – http://www.aksimed.ru/download/center/Bazovaya-model.pdf (дата обращения: 14.01.2014).

8. Wiener N. Cybernetics or Control and Communication in the Animal and the Machine. – New York: The Technology Press and John Wiley & Sons, Inc. – Paris: Hermann et Cie, 1948.

9. Internal Threats to America: Cyber & Intellectual Property Threat Study Guide Intellectual Takeout. – http://www.intellectualtakeout.org/sites/www.intellectualtakeout.org/files/Cyber%20Threats%20Study%20Guide%20-%20March%202012_2.pdf (дата обращения 28.12.2013).

10. Даник Ю.Г., Шестаков В.І., Чернишук С.В. Визначення сутності та змісту кібернетичної загрози // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. – 2012. – Спецвип. 2. – С. 5–14.

Даник Юрий Григорьевич, д-р техн. наук, профессор, начальник, Житомирский военный института им. С.П. Королева (г. Житомир); zvir@zvir.zt.ua.

Шестаков Валерий Иванович, канд. техн. наук, доцент, заместитель начальника по учебной и научной работе, Житомирский военный института им. С.П. Королева (г. Житомир); shvi@mail.ru.

Чернышук Сергей Викторович, адъюнкт, Житомирский военный института им. С.П. Королева (г. Житомир); chernuu@yandex.ru.

Поступила в редакцию 25 февраля 2014 г.

Bulletin of the South Ural State University
Series "Computer Technologies, Automatic Control, Radio Electronics"
2014, vol. 14, no. 2, pp. 52–60

APPROACH TO CYBERTHREATS CLASSIFICATION

***Danik Yu.G.**, Zhitomir Military Institute Named after S.P. Korolev, Zhitomir, Russian Federation, zvir@zvir.zt.ua,*
***Shestakov V.I.**, Zhitomir Military Institute Named after S.P. Korolev, Zhitomir, Russian Federation, shvi@mail.ru,*
***Chernyshuk S.V.**, Zhitomir Military Institute Named after S.P. Korolev, Zhitomir, Russian Federation, chernuu@yandex.ru*

Majority of modern researchers consider cyberthreats to citizen, society and whole country in context of information security or data protection and don't take into account peculiarities of management processes witch take place in information systems.Purpose of this paper is to develop existing approaches to cyberthreats classification with regard to management process peculiarities. It's suggested to consider cyberthreats as threats to management processes on different levels, existing classifications of cyberthreats are supplemented with most important features for defense and counteraction, possibility of sug-

gested classification scheme practical application for information and control systems is demonstrated. Achieved results allow to systematize existent in this subject area knowledge for their further appliance in cyberthreats modeling and development of methods and countermeasures for cyber security of citizens, society and whole country.

Keywords: cybersecurity, cyberthreat, classification.

References

1. National Cyber Security Strategies in the World. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (accessed 09.01.2014).

2. Osnovnye napravleniya gosudarstvennoy politiki v oblasti obespecheniya bezopasnosti avtomatizirovannykh sistem upravleniya proizvodstvennymi i tehnologicheskimi protsessami kriticheski vazhnykh ob'ektov infrastruktury Rossiyskoy Federacii [The Main Directions of a State Policy in the Security Field of Automated Control Systems by Production and Technological Processes of Infrastructure Crucial Objects]. Available at: http://www.scrf.gov.ru/ documents/6/113.html (accessed 05.08.2013).

3. Kornjushin P.N., Kosterin S.S. Informacionnaya bezopasnost' [Information Security]. Vladivostok, TIDOT DVGU, 2003. 154 p.

4. Buryachok V.L., Gulak G.M., Horoshko V.O. [Tasks, Forms and Methods of Warfare in Cyberspace]. *Nauka i oborona* [Science and Defense], 2011, no. 3, pp. 35–42. (in Ukrainian)

5. Golovan' V.G., Drozdov O.M., Sergeev V.V., Gerasimov V.M. [Information Security of the Power: Aspect of Information and Psychological Threats]. *Problemi stvorennja, viprobuvannja, zastosuvannja ta ekspluataciї skladnih informacijnih sistem: zb. nauk. prac'* [Problems of complex information systems development, research, appliance and exploitation], 2011, no. 5, pp. 33–41. (in Ukrainian)

6. Konev A.A. [Approach to Development of Threat Models for Secured Information]. *TUSUR Reports*, 2012, no. 1 (25), part 2, pp. 34–40. (in Russ.)

7. *Bazovaja model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh* [Basic Model of Security Risks of Personal Data in Case of their Processing in Personal Data Information Systems]. Available at: http://www.aksimed.ru /download/center/Bazovaya-model.pdf (accessed 14.01.2014).

8. Wiener N.Cybernetics or Control and Communication in the Animal and the Machine. New York, The Technology Press and John Wiley & Sons, Inc., Paris, Hermann et Cie, 1948.

9. Internal Threats to America: Cyber & Intellectual Property Threat Study Guide Intellectual Takeout. Available at: http://www.intellectualtakeout.org/sites/www.intellectualtakeout.org/files/Cyber%20Threats%20Study%20Guide%20-%20March%202012_2.pdf (accessed 28.12.2013).

10. Danyk Y.G., Shestakov V.I., Chernyshuk S.V. [Determination of CyberthreatsEssence and Content]. *Problemi stvorennja, viprobuvannja, zastosuvannja ta ekspluataciї skladnih informacijnih sistem: zb. nauk. prac'.* [Problems of complex information systems development, research, appliance and exploitation], 2012, pp. 5–14. (in Ukrainian).

Received 25 February 2014