УДК 681.324.067

Геном информатизации и корпоративная иммунология интернета

Осовецкий Л. Г.

Постановка задачи. *Лавинообразное развитие сети Интернет, как комплекса взаимоувязанных программных средств корпоративных сетей, актуализирует вопросы обеспечения безопасности Интернет, как единой сложной системы.* ***Цель работы.*** *В статье ставится проблема функциональной безопасности Интернет как комплекса программных средств корпоративных сетей, влияющих на безопасность пользователей.* ***Используемые методы.*** *Для оценки функциональной безопасности Интернет в статье выделены факторы, наибольшим образом влияющие на факторы, определяющие уязвимость Интернета, рост объемов мертвого кода.* ***Новизна работы.*** *Функциональная безопасность комплекса программ Интернет рассмотрена с точки зрения корпоративных пользователей, при этом использована аналогия развития информационных технологий с эволюцией информационной генетической системы человека. Для детализации требований по функциональной безопасности Интернет целесообразно использовать аналогию построения информационно-программных систем Интернет с информационной генетической системой живых организмов, а системы защиты и безопасности информации – с построением иммунной системы живых организмов.* ***Результаты.*** *Показано, что безопасность Интернета, как комплекса программных средств, определяется минимизацией уязвимостей используемых программ и степенью защищенности корпоративных сетей, функционирующих в составе Интернет. Характеристики и показатели информационной безопасности отдельных программных средств и крупных комплексов программ в составе сети Интернет существенно отличаются. Нормативные документы по требуемым показателям защищенности и безопасности информации, должны учитывать фактор различной размерности функционального программного обеспечения.*

Ключевые слова: *безопасность, Интернет, корпоративные системы, угрозы, уязвимость, геном, популяция.*

Введение

Важнейшей проблемой, определяющей темпы и будущее развитие Интернета, становится информационная безопасность. Глубокое проникновение компьютерных информационных технологий (ИТ), телекоммуникационных технологий (ИКТ), Интернет во все сферы человеческой деятельности и многочисленные проблемы в их защите требуют более широкого внедрения защищенных информационных технологий. Уже сегодня информационные технологии являются «нервной системой» каждого развитого государства и мира в целом, которая позволяет функционировать остальным его подсистемам. А ядром всей информационной инфраструктуры становится сеть Интернет. В настоящее время сеть Интернет объединяет миллионы компьютеров во всем мире. Эти же компьютеры контролируют реальные физические объекты такие как, электрические станции, поезда, химические реакции, радары, сырьевые рынки, которые сами находятся вне пространства сети Интернет. Таким образом, ИТ, ТКС, Интернет становятся критическими информационными технологиями, способными влиять на национальную безопасность отдельных стран и мира в целом.

Правительства развитых стран, чьи экономика и национальная безопасность уже в настоящее время находятся в сильной зависимости от информационных технологий и информационной инфраструктуры, осознают надвигающуюся опасность и предпринимают соответствующие контрмеры. Понимание важности вопросов безопасности глобальных телекоммуникационных технологий Правительством России нашло отражение в Доктрине Информационной Безопасности РФ от 9 сентября 2000 года, отражающей совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Отмечено, что одним из основных методов обеспечения информационной безопасности в РФ является «формирование **системы мониторинга** показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства». Проводится разработка новой версии Доктрины.

Следует учитывать, что глобальное развитие информационных технологий и Интернета в мире несет не только положительный эффект. Их рост и применение влечет за собой угрозы не только информационной безопасности людей, но и существенно влияет на эволюционное развитие человечества в целом, в том числе и отрицательное. Появились и прогрессируют новые понятия в области безопасности. Это киберпреступность и кибербезопасность, вирусная активность, несанкционированный доступ к информации и кибершпионство, информационные войны и киберустойчивость.

Это влияние ИТ, ТКС и Интернета на жизнь людей при увеличении новых вариантов угроз безопасности заставляет задуматься о перспективах и источниках их появления. Представление о том, что ИТ, ТКС и Интернет – порождение человека, а не природы, и поэтому полностью находится под управлением человека, не выдерживает критики. Эти объекты сегодня представляют по размерности огромные и быстро растущие образования, до сих пор не встреченные в эволюции человека. Они влияют на жизнь людей и в положительном и в отрицательном аспекте.

Они по своей сути являются очередным шагом эволюции человеческой популяции в части развития популяционной информационной системы. Базой, источником и аналогом такой информационной системы в природе является генетическая информационная система человека [1].

Положительные прогнозы развития Интернета и ИТ в основном исходят от торговых и финансовых организаций и фирм, базирующиеся на надеждах роста финансовой прибыли. Ряд отрицательных прогнозов исходят от специалистов в области информационных технологий и защиты информации.

Все эти прогнозы [1] базируются на основе статистики по недолговременной истории развития ИТ и Интернета и не учитывают системную популяционную составляющую, которая более важна для эволюции человечества в целом.

Развитие и эволюция информационной системы Интернета сравнима с развитием природной информационной генетической системы человека,

которая по количественным параметрам пока превышает количественные параметры развития ИТ и Интернета.

Однако темпы роста Интернета и его влияния на эволюцию популяции человека заставляют анализировать и прогнозировать его развитие на основе этой аналогии.

Для оценки влияния Интернета на развитие и эволюцию человека следует проанализировать и сравнить количественные характеристики эволюции информационных систем.

На рис. 1 представлены сравнительные оценки объемов накопленной и хранимой информации, темпов обмена информацией между информационными объектами генетической системы человека, информационной системой человека (условно мозгом человека) и ИТ, ТКС, Интернетом. Объем хранимой информации в Интернете сейчас гораздо меньше информационных систем человека, однако, темп роста объема накопленной информации составляет более чем двукратное ее увеличение в течение года. Темпы роста накопленной человеком информации связаны с ростом общей численности людей на Земле и требуемым ростом объема информации генетической системы человека что, по-видимому и является объективной причиной необходимости использования Интернета в дальнейшей эволюции человечества.

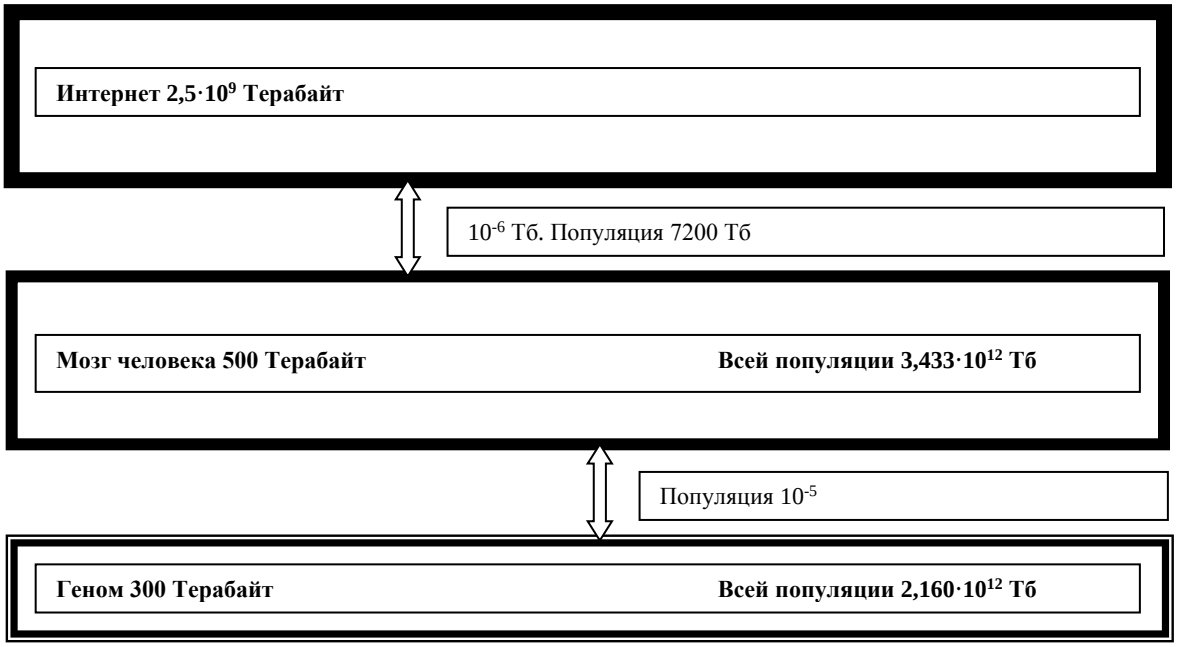


Рис.1. Оценки объемов и скорости обмена информацией между объектами

Часто бытующие представления о том, что информатика и ее развитие не влияют на развитие отдельных людей и человечества в целом, подлежит пересмотру и сравнительному анализу с эволюцией формализованной информационной генетической системы. В настоящее время наиболее существенно то, что человечество переживает демографический переход [2]. Одной из причин достижения демографического перехода роста численности населения мира может являться неспособность накопления и обмена

информационными ресурсами имеющимися способами между членами популяции, что и привело к появлению Интернета и ИТ для продолжения дальнейшей эволюции популяции человека.

На рис. 2 [1] представлена динамика роста численности населения мира по исследованиям Сергея Петровича Капицы (и, соответственно, количественные характеристики информационной генетической системы человеческой популяции). На рис.2 цифрой 1 обозначено мировое население, 2 – режим с обострением, 3 – демографический переход, 4 – стабилизация населения, 5 – древний мир, 6 – средние века, 7 – новая и 8 – новейшая история, стрелка указывает на период чумы – "Черная смерть", кружок – настоящее время, двухсторонняя стрелка – разброс оценок численности населения мира при Рождестве Христовом (Р.Х.). Предел населения N_∞=12–13 млрд.

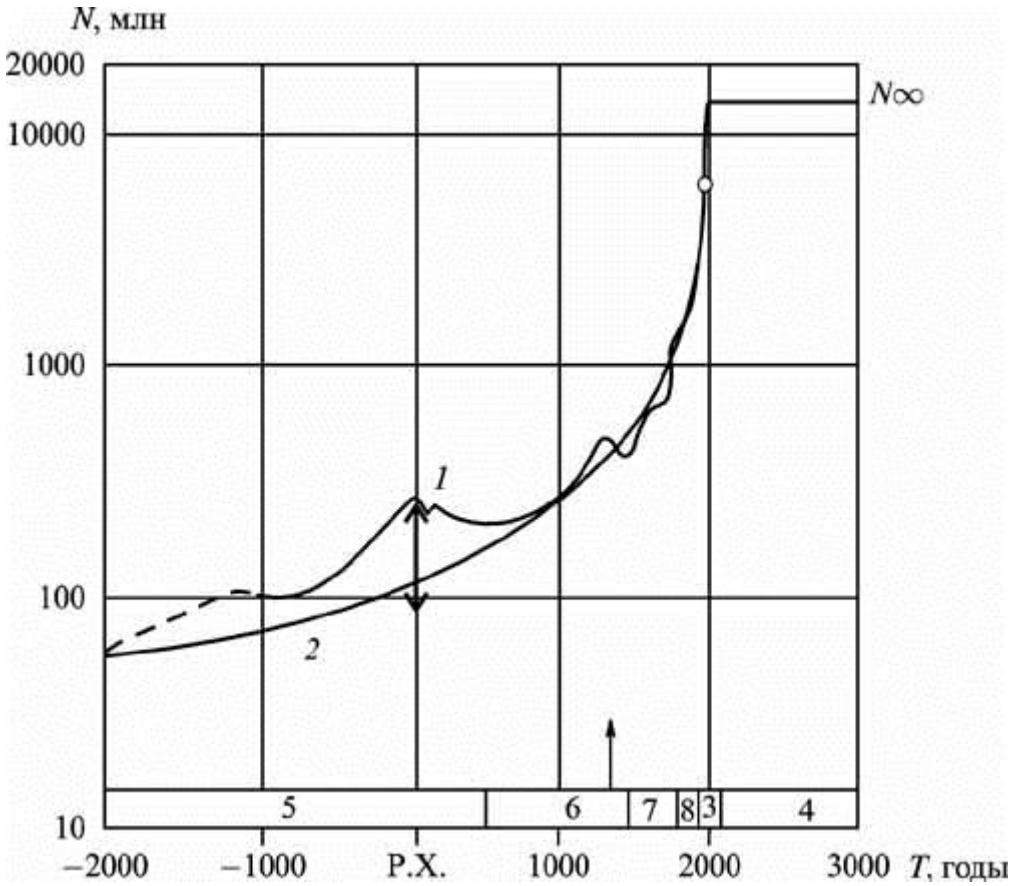


Рис. 2. Население мира от 2000 г. до н.э. до 3000 г.

Эволюция биологической информационной системы длилась 4000 лет [2]. Развитие Интернета и ИТ происходит в течении 50 лет, что примерно в 80–100 раз меньше. По временному параметру сравнение на основе используемой аналогии не проходит. Если с системной точки зрения принять, что число пользователей Интернет пропорционально объему накопленной и циркулирующей информации, то сравнение по численности (информационному объему) человеческой популяции и популяции пользователей Интернет (3–5 млн) показывает, что приближается момент совпадения численности членов обеих популяций.

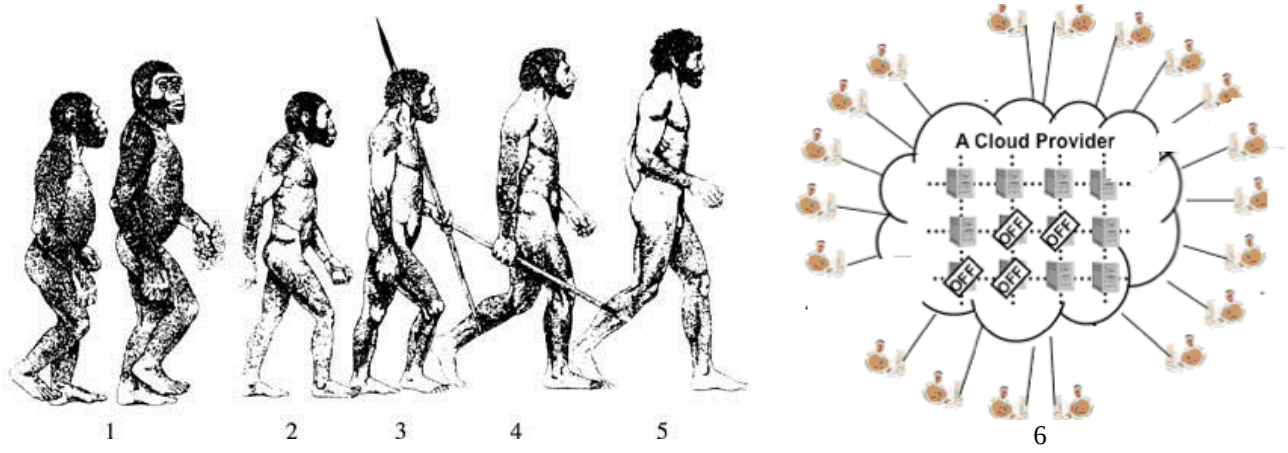
Это позволяет использовать другие параметры сравнения.

Ход кривой роста пользователей Интернета аналогичен ходу кривой роста численности населения. Это позволяет предположить, что предел численности пользователей Интернета естественно будет ограничен численностью населения, т. е. 12–15 млрд.

Этот предел, с учетом изменения и перерасчета временных масштабов, может быть достигнут к 2100 году.

После достижения предела численности пользователей, Интернет и ИТ ожидает «демографический информационный переход», что влечет за собой необходимость поиска новых средств и способов накопления и обмена информацией.

Попытки прогноза развития Интернета и ИТ на основе приведенных данных заставляют предположить, что в антропогенезе человека наступила стадия Humanity Sapiens – человечество разумное (рис. 3), которая характеризуется коллективным наполнением базы данных и знаний и коллективным их использованием.



1 – австралопитек, 2 – Homo Habilis, 3 – питекантроп, 4 – Homo Sapiens (неандерталец), 5 – современный человек, 6 – Humanity Sapiens

Рис. 3. Стадии антропогенеза

С точки зрения эволюции человека, по-видимому следует ожидать поиск и создание средств хранения информации с увеличением объема накапливаемых данных, ускорения и упрощения доступа к ним отдельным членам популяции, обеспечения достоверности данных, исключения вредоносных действий источников информации – интеграции использования информационных ресурсов.

Эта же тенденция, по-видимому будет развиваться в использовании Интернета и ИТ.

Технология и эволюция развития популяций (в том числе Интернета) существенно отличаются от принципов развития отдельных членов популяции [4]. Как показано Эйгеном и Шустером, в эволюции популяций существенны три процесса: мутация (изменение отдельного члена популяции, зависящее от его качества), тиражирование – копирование и размножение члена популяции

(зависит от уровня качества члена популяции), удаление члена популяции (при уменьшении его качества).

Изучение и прогнозирование развития Интернета с позиций развития человеческой популяции наиболее перспективно и полезно и для Интернета, и для человечества в целом. Такой анализ показывает, что дальнейшее развитие Интернета базируется, в первую очередь, на организации механизмов и технологии защиты и безопасности информации (иммунологии ИТ) и внедрении новых видов обмена информацией, отличающихся от существующих достоверностью и качеством.

Иммунология Интернет и корпоративное представление пользователей

С точки зрения пользователя, Интернет представляет собой огромный комплекс взаимодействующих программ с разнообразными функциями. В то же время, в практике разработок ответственного программного обеспечения сформировался достаточно полный перечень требований, определяющий функциональную безопасность таких ответственных программ. Если оценивать Интернет с этой точки зрения, то это позволит обеспечить его функциональную безопасность для пользователей. Однако, оценить безопасность всего комплекса программ Интернет пока не представляется возможным.

Основные негативные стороны использования Интернета связаны с безопасностью его использования. Несмотря на это, международные стандарты по качеству программного обеспечения Интернет не определяют разницы между безопасностью отдельных программ и Интернета.

Стандартизированные в ISO 9126:1-4:2002 и уточненные в ISO 25010:2011 показатели безопасности не учитывают существенные отличия отдельных программ от их конгломерата в Интернете. Отечественные стандарты по безопасности и защите информации (РД АС и РД СВТ ФСТЭК России) [5, 6] также не содержат различные требования по безопасности и защите информации в зависимости от уровня сложности программного объекта.

Безопасность программного обеспечения в Интернет – очень широкое понятие, включающее экономическую, техническую, экологическую, социальных процессов и многие другие области человеческой деятельности. Это понятие отражает состояние использования комплекса программ Интернета, при котором отсутствует недопустимый риск, связанный с причинением вреда пользователю [2].

При попытке использования этого понятия к комплексу программ Интернет, возникает ряд вопросов.

Интернет – многопользовательский (многосубъектовый) комплекс программ, в котором существуют пользователи и группы пользователей, конкурирующие в части достижения своих целей, иногда противоречащие целям других пользователей или их групп. Часть пользователей преследует зловредные цели по несанкционированному доступу к информации других пользователей.

Что является недопустимым риском при использовании Интернет?

Число атак несанкционированного доступа прогнозируется не менее чем по одной атаке на компьютер в день. Не каждая атака приводит к реализации атаки, но при планомерном исследовании выбранного для атаки компьютера каждая неудавшаяся атака приводит к приближению результативности атаки, то есть к увеличению вероятности несанкционированного доступа.

Рассмотрим комплекс компьютеров из одного миллиона компьютеров. Если все компьютеры из указанного числа не связаны между собой, то потеря одного компьютера не влияет на работоспособность всей системы, вся система в целом достаточно защищена.

Если представить себе комплекс одного миллиона компьютеров, взаимосвязанных в корпоративные сети из 1000 компьютеров, а частота реализованных атак НСД составляет 10^{-6}, то вероятность НСД к информации к каждому компьютеру в такой системе составляет 10^{-3}, то есть взломана будет только одна корпоративная сеть, а остальные не пострадают.

Если численность корпоративных сетей достигает уровня 10 млн. компьютеров, то в каждой корпоративной сети появляются несколько взломанных компьютеров, что делает нежизнеспособной всю систему корпоративных сетей в Интернете.

Расчеты показывают, что уже в такой десяти миллионной системе взаимосвязанных компьютеров количество конкурирующих корпоративных сетей численностью более сотни компьютеров составляет более тысячи и при существующей частоте атак НСД взлом превышает допустимые нормы для гарантий безопасной работоспособности корпоративных сетей.

Приведенная оценка безопасности программного обеспечения в Интернет показывает, что нормативные документы по безопасности должны быть доработаны в части учета уровня сложности корпоративных сетей и подходов к построению адекватных систем защиты и безопасности информации.

Постоянно меняющийся состав программ в Интернете и увеличение количества пользователей функционирования Интернета приводит к тому, что невозможно предсказать заранее качество функционирования, и вероятны различные аномалии, завершающиеся отказами, отражающимися на безопасности. Необходимо признать принципиальные трудности аналитического оценивания и прогнозирования значений функциональной безопасности Интернета вследствие непредсказуемости проявления и последствий действия угроз безопасности. Это приводит к практической невозможности достоверных априорных аналитических расчетов функциональной безопасности Интернета [2, 3, 4].

Безопасность Интернета в большинстве случаев определяется не только факторами причинения вреда пользователю, но и возможностью реализацией этих факторов, то есть Угрозами безопасности.

Угрозы безопасности с точки зрения используемых программных продуктов определяются их уязвимостью – наличием в их конструктивной реализации мест и возможностей реализации угроз безопасности [11, 12].

Одними из таких часто используемых угрозами безопасности мест уязвимости является мертвый код.

Мертвый код

Рассмотрим небольшой пример, на рис. 4 изображена схема, моделирующая бизнес-процесс обработки кредитной информации [9].

Для осуществления последнего действия нам необходимо на основе полученной информации выбрать минимальную ставку по кредиту (рис. 5).

Рассмотрим ситуацию, когда выбор происходит из трех вариантов параллельно другим процессам (то есть структура проверки условий должна быть последовательной, чтобы это не повлияло на другие действия).

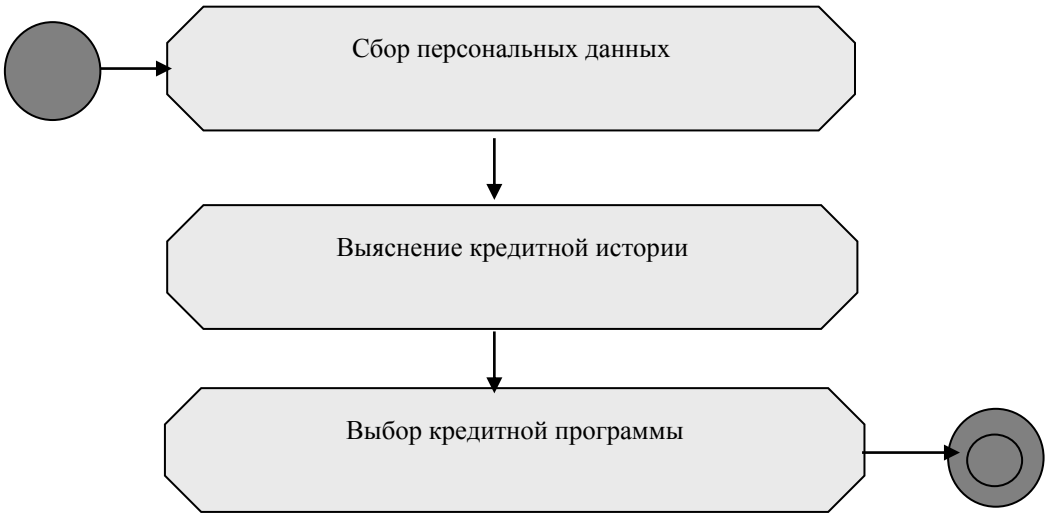


Рис. 4. Сбор данных

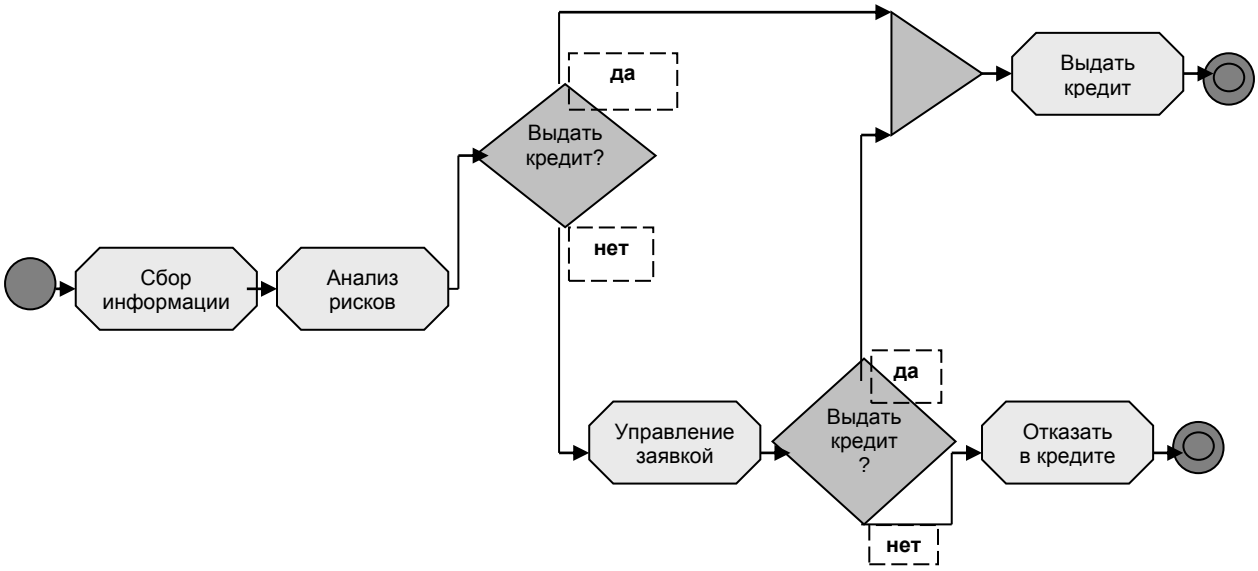


Рис. 5. Выбор кредитной программы

Пусть условие α: $x_1 < x_2$, β: $x_2 < x_3$, а γ: $x_1 < x_3$. Так же особо обговорено, что $x_1 \neq x_2$, $x_1 \neq x_3$ и $x_2 \neq x_3$ (так как мы рассматриваем программы кредитования и при равенстве ставок не имело бы смысла уделять внимание возможности выбора из нескольких вариантов). Результаты обозначим: λ_1: x_1 – минимальное значение, λ_2: x_2 – минимальное значение и λ_3: x_3 – минимальное значение. Тогда при их последовательной проверке мы придем к тому, что в некоторых случаях существуют такие пути, прохождение которых невозможно в силу несогласованности условий (рис. 6).

Из примера следует, что неисполняемая ветвь, которая впоследствии приведет к возникновению «мертвого кода» в тексте программы, может появиться на этапе формирования логической структуры, а это значит, что данную уязвимость следует распознавать именно на этом этапе, а не при формировании и тестировании кода, как принято считать.

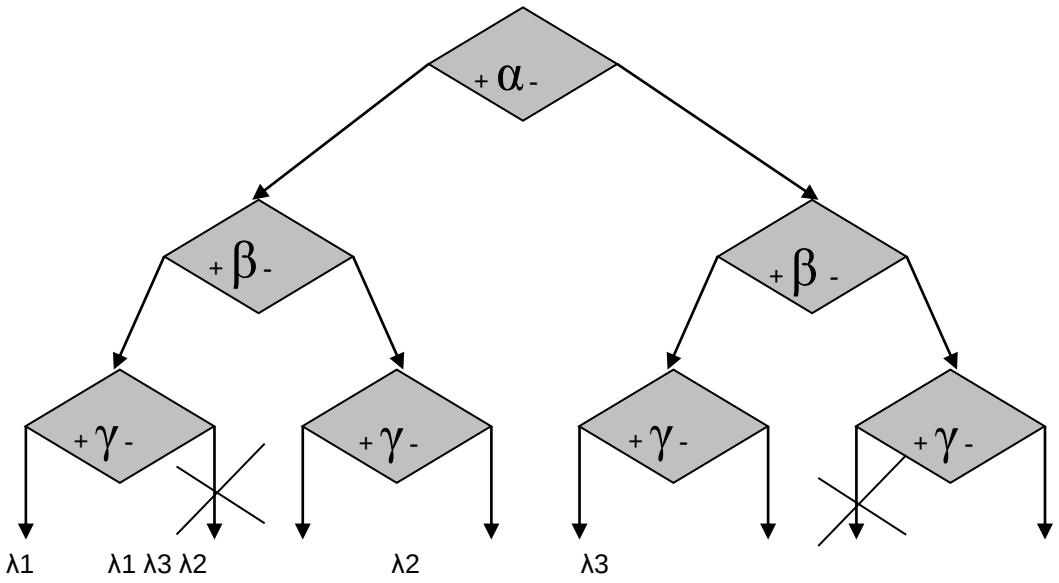


Рис. 6. Тупиковые пути при несогласованных условиях

Анализ объемов мертвого кода и, соответственно, уязвимостей программного обеспечения показывает, что рост объемов мертвого кода происходит с ростом объемов создаваемого программное обеспечение (ПО). При этом промышленное программное обеспечение, создаваемое с использованием инструментальных технологических средств промышленной технологии создания ПО, содержит еще большие объемы мертвого кода в связи с дополнительным внесением мертвого кода инструментальными технологическими средствами. Оценочный график роста объемов мертвого кода в зависимости от объемов разработки ПО приведен на рис. 7.

Структура корпоративного объединения пользователей в Интернет

Корпоративная сеть в теории защиты информации является временным объединением субъектов с единой целью оптимизации организации контроля над ресурсами, на которые претендуют также другие корпорации и субъекты, не входящие в рассматриваемую корпорацию. Формой объединения субъектов в корпорацию является использование единых для корпорации формальных

обозначений внешних объектов, то есть единого языка и наличие единой системы обмена информацией [9, 10]. В условиях существования достаточно большого числа возможных корпораций и вероятного их пересечения, сама информация становится ценным ресурсом, влияющим на текущее распределение контроля конкретных субъектов над использованием внешних ресурсов, и появлением конкуренции между корпорациями и субъектами за это распределение и стремления несанкционированного доступа к внутрикорпоративной информации со стороны других корпораций и субъектов. Указанный фактор приводит к одной из целей внутрикорпоративной информационной системы – организации защищенного обмена информацией, и к организации защищенного языка корпорации. Защищенность языка корпорации определяется, в первую очередь, защищенностью распределения ключевой информации, а также контролем и поддержанием защищенности ключевой системы во времени, то есть к контролю субъектами корпорации целостности корпорации.

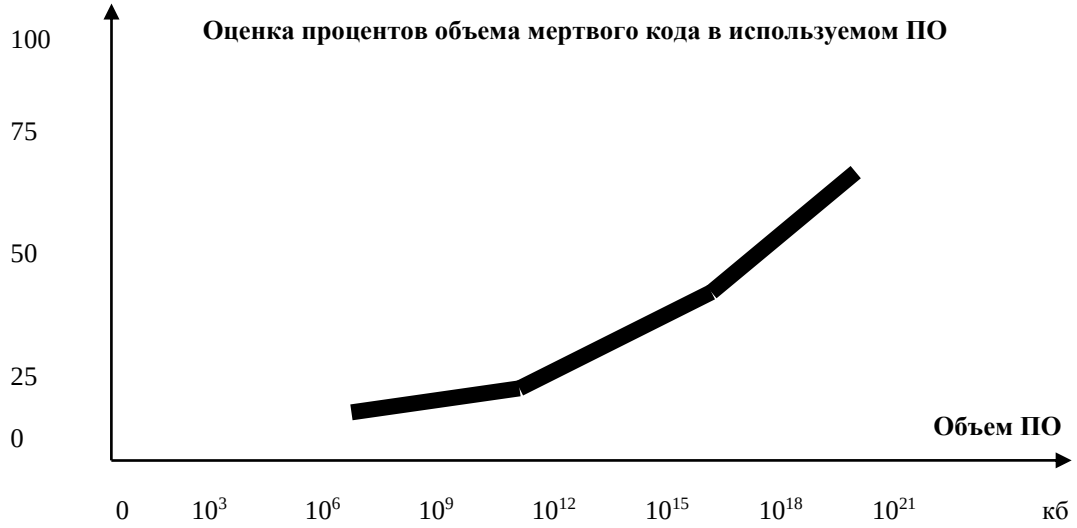


Рис. 7. Оценка объемов мертвого кода

Защищенные корпоративные сети образуются при помощи передачи контрольной информации между субъектами, которая бывает четырех видов: присоединение к корпорации (образование новых субъектов) и межкорпоративные взаимодействия (рис. 8).

Образование нового субъекта-члена корпорации – стрелка сверху вниз.

Образование членом корпорации нового субъекта – стрелка вниз.

Подключение внешним субъектом внутрикорпоративного субъекта к своей корпорации – стрелка слева направо.

Подключение членом корпорации внешнего субъекта – стрелка вправо.

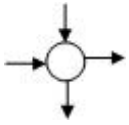


Рис. 8. Обозначение субъектов (членов корпорации) и их виды связей.

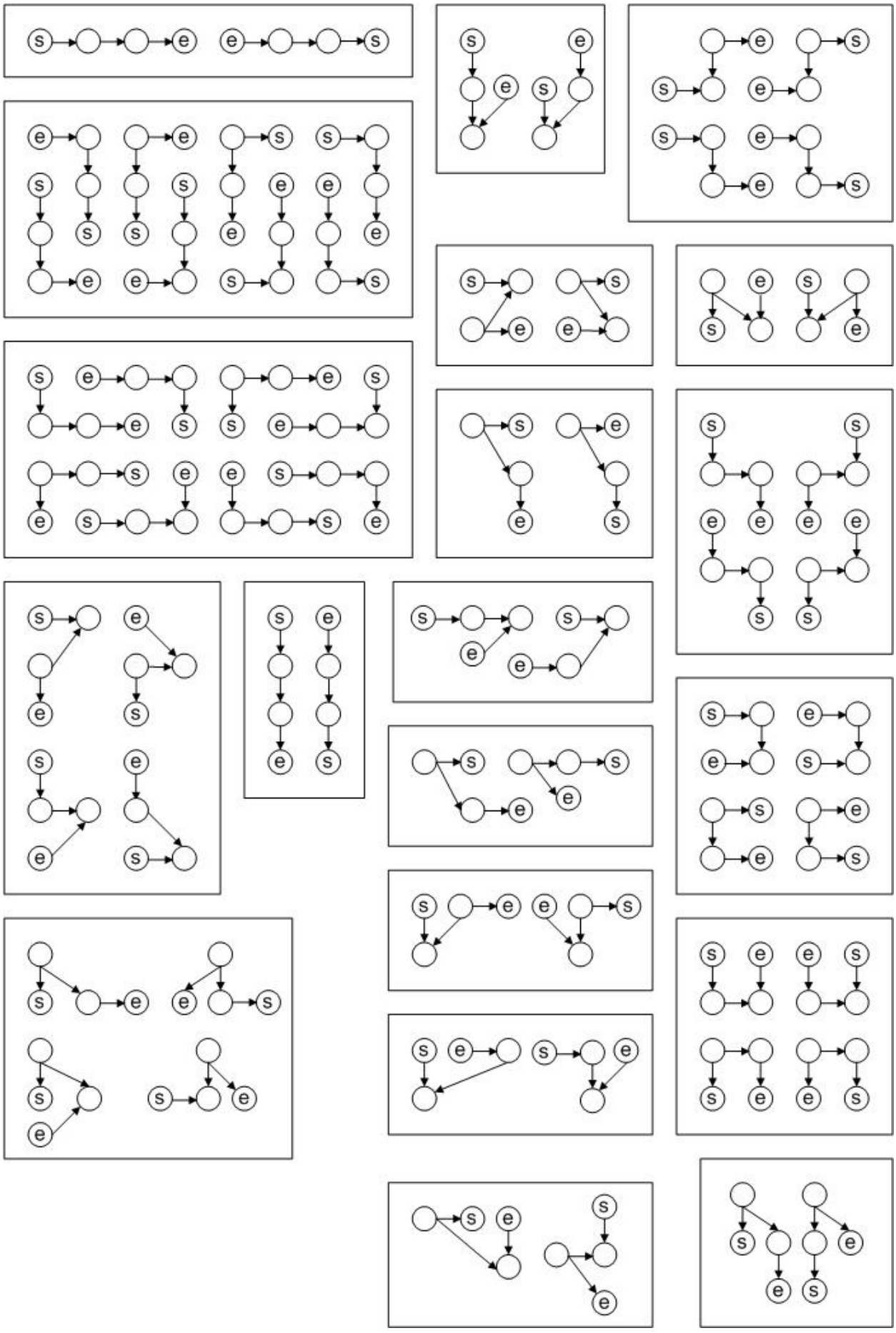


Рис. 9. Варианты блокирования 4-х субъектов корпорации тремя связями,

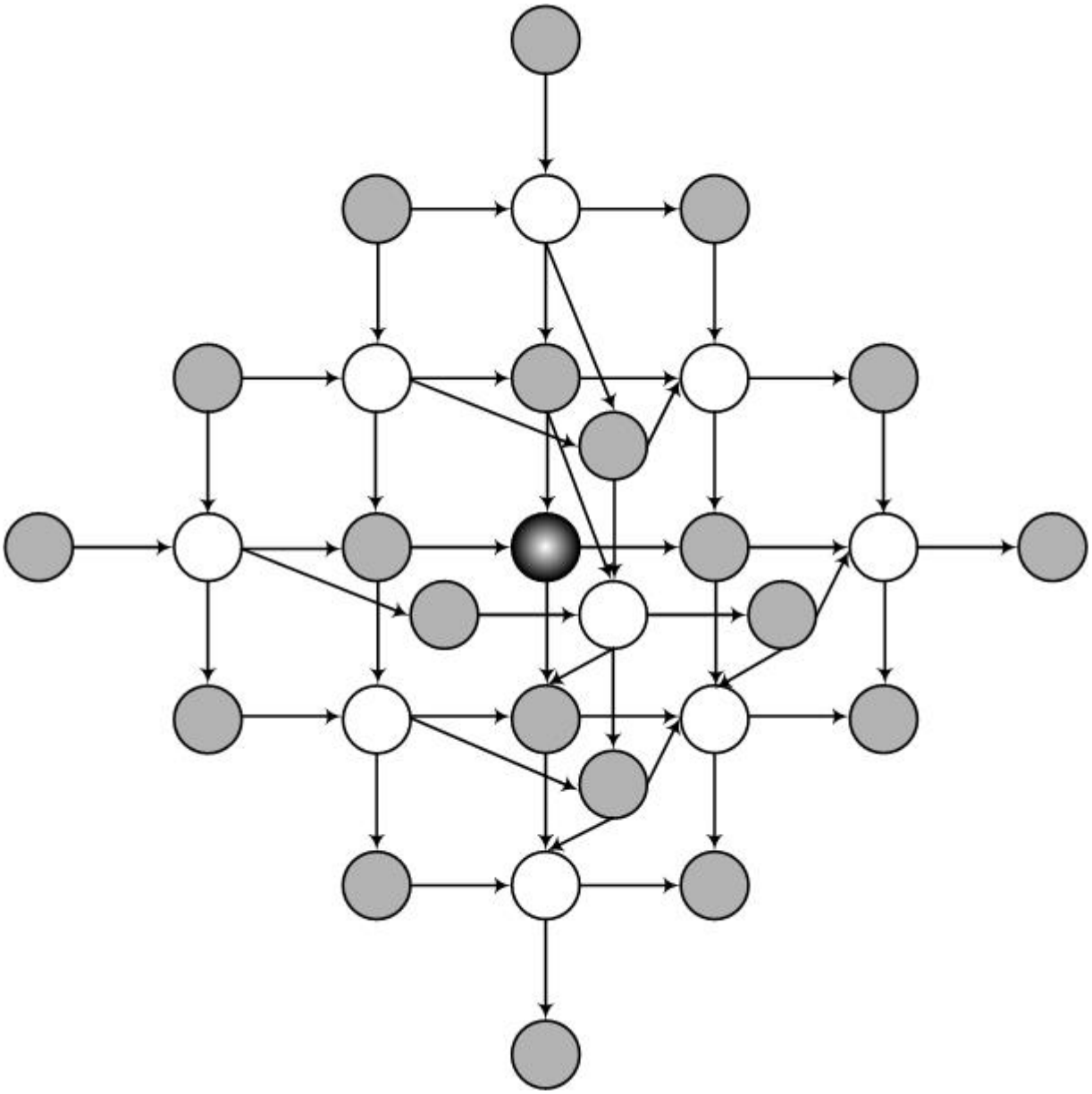


Рис. 10. Другой способ представления элементарных структур для описания ключевой системы, в результате которого возникают двадцать возможных положений оппонента, с которым субъект может быть связан тремя связями, обеспечивающими оптимальную защищенность ключевой системы между двумя субъектами S и E.

Защищенность всех возможных соединений (защищенность ключевой системы) между субъектами внутри корпорации и внешних соединений определяется степенью близости субъектов по параметру порождения ключевой системы субъектов. При возникновении обмена информацией между двумя субъектами возникает вопрос об определении их степени близости относительно друг друга. Для этой цели можно использовать набор связей, которые их логически объединяют, но такой подход не позволяет характеризовать степень близости субъектов, которая определяется всей предысторией развития корпорации. Расчеты показывают, что сравнение блокированных по две связи трех субъектов обладают максимальной близостью и, соответственно, защищенностью ключевой системы по сравнению с другими

видами блокирования по три и более связей для большего количества субъектов. Однако, для корпораций с числом субъектов более десятка, такая оценка не показательна, так как не позволяет провести сравнение близости и защищенности ключевой системы для достаточно удаленных членов корпорации.

При блокировании четырех субъектов с тремя связями возникает $4^3 = 64$ варианта связей, которые могут объединяться в двадцать блоков из соображений симметрии и качественно одинаковых структур по защищенности ключевой системы.

Таким образом, сама информационная сеть может кодироваться (представлена сочетаниями связей) четырьмя элементами, на основе которых для любых двух субъектов могут быть синтезированы цепочки из двадцати видов сочетаний, которыми просто оценивать отношения близости между субъектами.

Необходимо отметить аналогию такого подхода с кодированием белка в живой природе (см. рис. 9, рис. 10) В природе белок состоит из двадцати аминокислот. Каждая аминокислота представлена в составе ДНК в виде триплетов – три нуклеотида, по четыре знаковых вида. То есть триплетов всего 64, но кодируют они 20 аминокислот [7, 8, 9].

Приведенный анализ показывает, что в современных корпоративных системах, насчитывающих тысячи субъектов, определяющим фактором их существования и развития является наличие защищенной системы обмена информацией, базирующейся на эффективной языковой системе с гарантированной защищенностью ключевой системы. Максимальную защищенность на нижнем языковом уровне (уровне системы команд) обеспечивает четырехзначное кодирование триплетов, порождающих 20 видов команд.

Совпадение результатов приведенного анализа со структурой кодирования генетического кода живых организмов показывает, что и для этой корпоративной системы, определяющим фактором системы эффективного кодирования является не помехоустойчивость, а защищенность языковой системы.

Выводы

Безопасность Интернета как комплекса ответственных программных средств определяется минимизацией уязвимостей используемых программ и степенью защищенности корпоративных сетей, функционирующих на базе Интернета.

Литература

1. Осовецкий Л. Г., Немолочнов О. Ф., Твердый Л. В., Беляков Д. А. Основы корпоративной теории информации. СПб: СПбГУ ИТМО, 2004.

2. Кантышев П., Сальманов О., Шляпникова О. Угроза кибертерроризма – это печальная реальность // Ведомости. IT-бизнес. № 3972. 02.12.2015. URL:

http://www.vedomosti.ru/technology/characters/2015/12/02/619223-ugroza-kiberterrorizma.

3. Капица С. П. Общая теория роста человечества: Сколько людей жило, живёт и будет жить на Земле. М.: Наука, 1999.

4. Вернадский В. И. Живое вещество. М.: Наука, 1978. 350 с.

5. Эйген М. Самоорганизация материи и эволюция биологических макромолекул. М.: Мир, 1973. 214 с.

6. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992.

7. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности и требования по защите информации». Решение председателя Гостехкомиссии России от 30 марта 1992.

8. Карасев В. А. Генетический код: новые горизонты. СПб.: ТЕССА, 2003. 146 с.

9. Твердый Л. В. Метод защищенного распределения управляющих реквизитов СЗИ в межкорпоративных сетях: диссертация ... кандидата технических наук: 05.13.19. СПб: Университет ИТМО, 2008. 105 с.

10. Кукушкин Н. С., Меньшиков И. С., Меньшикова О. Р., Моисеев Н. Н. Устойчивые компромиссы в играх со структурированными функциями выигрыша // Журнал вычислительной математики и математической физики. 1985. Т. 25. № 12. С. 1761-1776.

11. Осовецкий Л. Г., Торшенко Ю. А. Источники «мертвого кода» при использовании технологии IBM Rational. Научно-Технический Вестник Университета Информационных технологий, механики и оптики. 2008. Т. 8. № 7(52). С. 184-187.

12. Осовецкий Л. Г., Немолочнов О. Ф., Твердый Л. В., Беляков Д. А. Основы корпоративной теории информации. СПб: Издательство СПбГУ ИТМО, 2004.

13. Липаев В. В. Надежность и функциональная безопасность комплексов программ реального времени. М.: Высшая школа, 2013. 207 с.

References

1. Osovetskiy L. G., Nemolochnov O. F., Tverdyiy L. V., Belyakov D. A. *Osnovyi korporativnoy teorii informatsii* [The Corporate Foundations of Information Theory]. St. Petersburg, ITMO University Publ, 2004 (in Russian).

2. Kantyshev P., Sal'manov O., Shliapnikova O. Ugroza kiberterrorizma – eto pechal'naia real'nost'. *Vedomosti. IT-biznes*, no. 3972, 01.12.2015. Aviliable at: http://www.vedomosti.ru/technology/characters/2015/12/02/619223-ugroza-kiberterrorizma (in Russian).

3. Kapitsa S. P. *Obschaya teoriya rosta chelovechestva: Skolko lyudey zhilo, zhivYot i budet zhit na Zemle* [A General Theory of Growth of Humankind: How

Many People Lived, Lives and will Live on Earth]. Moscow, Nauka, 1999 (in Russian).

4. Vernadskiy V. I. *Zhivoe veschestvo*[Living Matter]. Moscow, Nauka Publ., 1978. 350 p. (in Russian).

5. Eigen M. Selforganization of Matter and the Evolution of Biological Macromolecules. *Naturwissenschaften*, 1971, vol. 58, no. 10, pp. 465-523.

6. *Rukovodyaschiy dokument. Avtomatizirovannyie sistemyi. Zaschita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannyih sistem i trebovaniya po zaschite informatsii* [Protection against unauthorized access to information. Automated systems classification and requirements for protection of information. Russia Standard]. Reshenie predsedatelya Gostehkomissii Rossii ot 30 marta 1992 (in Russian).

7. *Rukovodyaschiy dokument. Sredstva vyichislitelnoy tehniki. Zaschita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zaschischennosti i trebovaniya po zaschite informatsii* [Computer equipment. Protection against unauthorized access to information. The security metrics and requirements for data protection. Russia Standard]. Reshenie predsedatelya Gostehkomissii Rossii ot 30 marta 1992 (in Russian).

8. Karasev V. A. *Geneticheskiy kod: novyie gorizontyi.* [Genetic Code: New Horizons]. Saint-Petersburg, TESSA Publ., 2003. 146 p. (in Russian).

9. Tverdyiy L. V. *Metod zashchishchennogo raspredeleniia upravliaiushchikh rekvizitov SZI v mezhkorporativnykh setiakh*. Diss. kand. tehn. nauk [Method of Protected Distribution of Control Details of GIS in Intercorporate Networks. Ph.D. Tesis]. Saint Petersburg, ITMO University Publ., 2008. 105 p. (in Russian).

10. Kukushkin N. S., Men'shikov I. S, Men'shikova O. R.,.Moiseyev N. N. Stable Compromises in Games with Lattice Payoff Functions. *USSR Computational Mathematics and Mathematical Physics*, 1985, vol. 25, issue 6, pp. 108-116.

11. Osovetskiy L. G., Torshenko Yu. A. Istochniki «mertvogo koda» pri ispolzovanii tehnologii IBM Rational [Sources of "Dead Code" when Using IBM Rational]. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*. 2008, vol.8, no 7(52), pp. 184-187 (in Russian).

12. Osovetskiy L. G., Nemolochnov O. F., Tverdyiy L. V., Belyakov D. A. Osnovyi korporativnoy teorii informatsii [Fundamentals of Corporate Information Theory]. Saint-Petersburg, ITMO University Publ., 2004 (in Russian).

13. Lipaev V. V. Nadezhnost i funktsionalnaya bezopasnost kompleksov programm realnogo vremeni [Reliability and Functional Safety of Software Real-Time Systems]. Moscow, Vyisshaya Shkola Publ., 2013. 207 p. (in Russian).

Статья поступила 6 декабря 2015 г.

Информация об авторе

Осовецкий Леонид Георгиевич – доктор технических наук, профессор, лауреат государственной премии совета министров СССР. Советник генерального директора. Ленинградское отделение Центрального научно-исследовательского института связи (ЛО ЦНИИС). Область научных интересов: информационная безопасность, безопасность программных средств. E–mail: leoned.osovetsky@gmail.com

Адрес: Россия, 196128, Санкт-Петербург, ул. Варшавская, 11.

Genome of Informatization and Corporate Immunology of Internet

L. G. Osovetskiy

Purpose. *The security of the Internet as set of software for corporate networks is an actual practical task. The Internet is represented as a joint complex system. The problem of functional safety the Internet as a set of software is studying in the paper. The security of the corporate network and user security affects on the safe of the Internet.* ***The methods used.*** *Factors influencing on the safety of the Internet, highlighted in the paper to assess its functional safety. Among these factors are highlighted - security software for corporate networks and the growth of dead code.* ***The novelty of the work****. Functional safety of Internet is examined from the point of view of safety of complex programs in corporate networks. In paper author used the analogy of development of information technologies with the evolution of the genetic system of humans. In the paper used the analogy of building information and software systems the Internet with the genetic system of living organisms and systems for the security of information - with the immune system of living organisms.* ***Results.*** *In the paper shows that the safety of Internet as set of software is determined by minimization of vulnerabilities of the used software and the level of protection of corporate networks in the Internet. Characteristics and indicators of information security separate software as part of network of the Internet differs considerably. Author offers new software for safe of Internet based on the immune concept of living organisms. Regulatory documents for the information security should consider it.* ***Practical relevance.*** *The results of the paper can be used to build the new complex systems information security of Internet which is based on immune principles of living organisms.*

Keywords: *security, Internet, enterprise systems, threats, vulnerabilities.*

Information about Author

Leonid Georgievich Osovetskiy – Dr. habil. of Engineering Sciences, Professor, Advisor of CEO of the Leningrad branch of the Central Science Research Institute of Communications (LO CNIIS). Leningrad Branch of Central Science Research Telecommunication Institute (LO ZNIIS). Field of research: information security, security software. E–mail: leoned.osovetsky@gmail.com

Address: Russia, 196128, Saint Petersburg, Varshavskaya str., 11.