УДК 681.3

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ОБЩЕСТВА И ИММУНОЛОГИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Л.Г. Осовецкий, д.т.н., профессор
(Ленинградское отделение Центрального научно-исследовательского института связи (ЛО ЦНИИС), leoned.osovetsky@gmail.com)

Аннотация. Ставится проблема перехода от использования разрозненных средств защиты информации в ИТ и ТКС к созданию иммунной системы защиты информации по аналогии с иммунной системой живых организмов. Рост сложности современных ПС ВС, их ответственности в критически важных вычислительных системах ставит новые задачи по качеству средств защиты и безопасности информации, обрабатываемой в них. Ближайшей аналогией СЗИ ВС становится технология СЗИ в биологических системах.

Ключевые слова: *иммунология, защита и безопасность информации, информационные технологии, телекоммуникационные технологии, генная инженерия.*

Человеческое сообщество получило новый мощный аппарат взаимодействия и дальнейшего развития – охватывающую все области жизни и деятельности человека структуру телекоммуникаций и автоматизированных вычислительных средств, расширяющих возможности в полезном обмене данными, скорости их использования в интересах личности, корпораций, государств.

Количественные характеристики объемов использования таких *информационных технологий* (ИТ) уже сравнимы с численностью популяции людей. По сути параллельно с человеческой популяцией развивается информационная телекоммуникационная популяция, получившая название информационного общества, причем вторая предназначена обеспечить развитие первой. Однако для позитивного влияния популяции ИТ на человеческую популяцию необходимы изучение, корректное знание и использование законов развития данных массовых систем. В противном случае, как это часто происходит при бездумном использовании людьми научных достижений, вместо пользы человеку наносятся ущерб и вред.

Аналогичная ситуация прослеживается и при анализе развития информационного общества. При высоком уровне эффективности использования ИТ в различных областях деятельности человека растет угроза безопасности и защиты информации. В результате реализации угроз наносится финансовый, моральный и физический ущерб пользователям, который сводит к нулю применение ИТ, а иногда имеет отрицательный эффект. Основная причина такой ситуации кроется в недооценке роста возможных потерь с повышением уровня сложности и использования современных ИТ. Поле угроз безопасности и защиты информации растет как по номенклатуре и содержанию, так и по интенсивности. В то же время методы и средства защиты и безопасности информации развиваются в среде новых ИТ на уровне создания отдельных защитных средств, ориентированных на защиту индивидуальных рабочих мест.

Система защиты и безопасности ИТ – это лишь часть общей проблемы безопасности нового для людей конгломерата человека и автоматизированных ИТ и *телекоммуникационных систем* (ТКС). Главной целью создания *системы защиты информации* (СЗИ) ИТ и ТКС остается безопасность пользователя в части все более увеличивающегося влияния на нее безопасности используемых ИТ и ТКС.

Исследования в области защиты и безопасности информации в информационных (ИТ) и телекоммуникационных (ТКС) технологиях начались по мере развития этих технологий. Они были обусловлены необходимостью обеспечения защиты на отдельных разнообразных технических и программных средствах ИТ и ТКС, вначале применяемых в государственных и банковских, а затем и в других структурах и получивших название критических. С повсеместным внедрением средств ИТ и ТКС для разнообразных целей, с развитием глобальной системы связи и обмена информацией Internet, потребовавшей унификации технических и программных средств ИТ и ТКС и персонализации этих средств, стало ясно, что критичность обрабатываемых и передаваемых данных является повсеместным и неотъемлемым свойством такой, все более сложной системы. Рост сложности ИТ и ТКС привел к качественному изменению представления о них. Из набора разрозненных технических и программных средств ИТ и ТКС превратились во взаимосвязанную взаимодействующую систему индивидуальных функциональных рабочих мест, имеющих унифицированный интерфейс для обмена информацией с другими рабочими местами системы, то

есть по сути в популяцию ИТ, законы развития которой существенно отличаются от законов развития разорванных изолированных рабочих мест. Образование популяции ИТ приводит, в частности, к резкому росту угроз безопасности и защиты информации. Соответственно, разрозненные индивидуальные средства защиты и безопасности информации должны стать системой коллективной популяционной защиты, методы и средства которой существенно отличаются от ранее существовавших. Наука защиты и безопасности информации в ИТ и ТКС должна превратиться в иммунологию ИТ и ТКС.

Используемая аналогия иммунологии ИТ с иммунологией живых организмов предусматривает признание того факта, что защита от многообразных угроз безопасности ИТ также должна носить многообразный, специализированный для каждого случая характер. Далее приведены некоторые модели и методы создания защиты и безопасности информации в ИТ и ТКС (иммунологии ИТ), не претендующие на полное и всеобъемлющее решение проблемы. В соответствии с используемой аналогией, которая должна приобрести конструктивный характер, приводятся примеры моделей наиболее перспективных, по мнению автора, аспектов перехода от решения локальных задач создания СЗИ ИТ к решению задачи создания иммунологии ИТ.

Искусственные иммунные системы как средство сетевой самозащиты

Системы, заимствующие у природы принцип иммунитета, называют *искусственными иммунными системами* (AIS – Artificial Immune System).

Специалисты, работающие в области AIS, отмечают три основных свойства иммунной системы человека: она является распределенной, самоорганизующейся, легковесной, то есть не особо требовательной к вычислительным ресурсам.

Именно этими свойствами, по мнению многих экспертов, должна обладать *система обнаружения вторжений в сеть* (IDS – Intrusion Detection System), которая по своим характеристикам приближалась бы к максимально эффективной.

IDS для одного сегмента сети, построенная на принципах искусственной иммунной системы, подразделяется на основную и набор вторичных. В основной IDS на базе AIS реализуются, а точнее имитируются, два процесса – эволюция генной библиотеки и *негативная селекция данных* (НСД) (рис. 1).

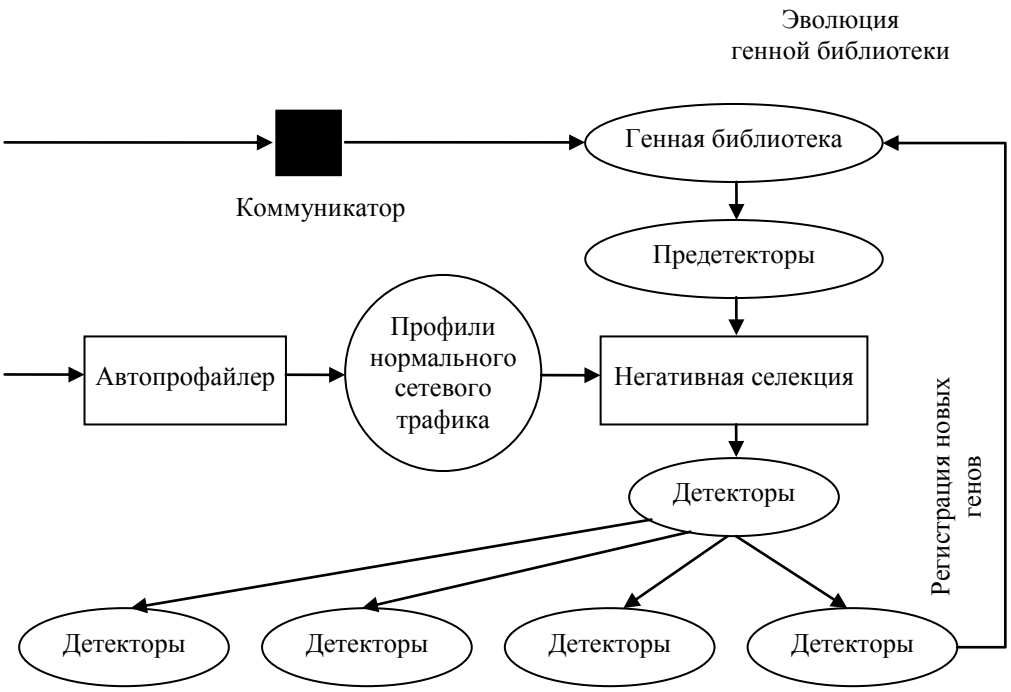

Рис. 1. Структура AIS

На этапе эволюции генной библиотеки происходит накопление информации о характере аномалий сетевого трафика. Генная библиотека искусственной иммунной системы должна содержать гены (данные о характерном количестве пакетов, их длине, структуре, типичных ошибках и т.д.), на основании которых будут генерироваться особые программные агенты – детекторы, служащие аналогами лимфоцитов. Начальные данные для формирования генной библиотеки выбираются исходя из особенностей применяемых сетевых протоколов, в частности, их слабых с точки зрения защиты мест. В дальнейшем при обнаружении детекторами аномальной активности в сети в библиотеку будут добавляться соответствующие этим проявлениям новые гены. Следует заметить, что, поскольку размер генной библиотеки ограничен, в ней сохраняются только наиболее часто проявляющиеся гены.

На втором этапе путем произвольного комбинирования генов происходит генерирование так называемых предетекторов, которые затем с помощью механизма негативной селекции проверяются на совместимость или на несовместимость с нормальным сетевым трафиком. При этом используются данные о характере такого трафика (профили), формируемые так называемым автоматическим профайлером, постоянно анализирующим поток данных, поступающий от маршрутизатора, стоящего на входе в сетевой сегмент.

Конечной целью в этом случае является создание ограниченного набора детекторов, с помощью которого можно было бы обнаружить максимальное число сетевых аномалий. Этот набор рассылается по узлам сети, образуя вторичную IDS.

Стоит отметить, что разработанные на сегодняшний день алгоритмы негативной селекции оперируют вероятностными характеристиками – вместо точного соответствия используется частичное, степень которого может произвольно варьироваться. Ее изменение, как нетрудно догадаться, в конечном итоге должно приводить к уменьшению или увеличению частоты ложных срабатываний.

При обнаружении аномалии соответствующий ей детектор размножается и рассылается на все узлы. Окончательное решение о том, происходит вторжение в сеть или нет, принимается на основании данных от нескольких узлов. Каждый узел, а также основная IDS снабжены еще одним компонентом – коммуникатором, который, в частности, оперирует таким параметром, как уровень риска. В случае, если на каком-то узле замечена подозрительная активность, коммуникатор поднимает свой уровень риска и отсылает

соответствующее сообщение коммуникаторам других узлов и основной IDS, которые тоже поднимают свои уровни риска. При появлении аномалий сразу на нескольких узлах в течение короткого промежутка времени этот уровень очень быстро растет, и, если будет достигнут заданный порог, администратор сети получит сигнал тревоги.

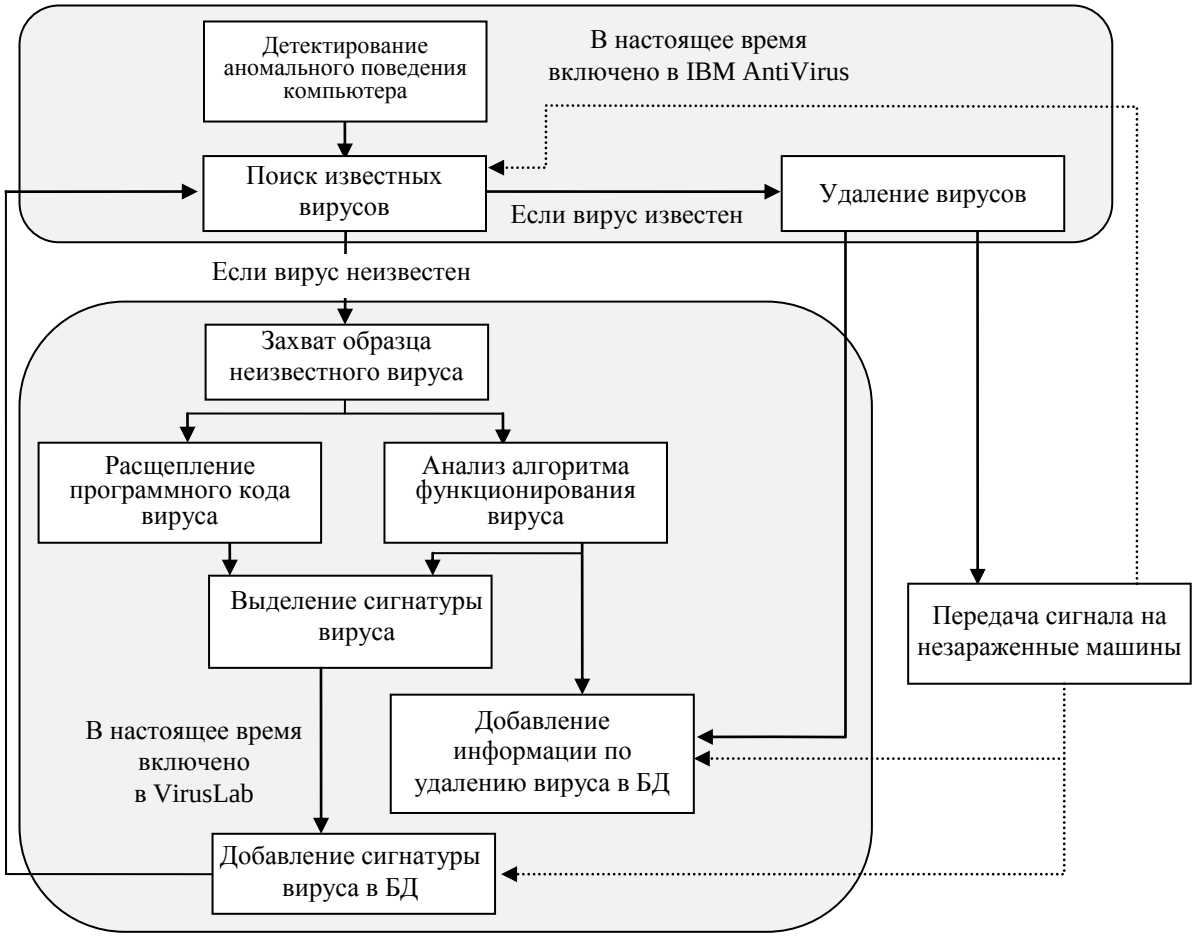

Рис. 2. Антивирусная технология на основе аналогии с иммунной системой человека

Двухпотоковая модель аутентификации субъекта в ИТ

Основным СЗИ при НСД является система аутентификации субъекта.

Двухпотоковая модель аутентификации использует множество обновляемых детектирующих наборов. От иммунной системы она наследует механизмы, позволяющие эффективно реагировать на действия злоумышленника, но при этом учитывает ограниченность возможностей искусственных систем защиты. Первый поток отвечает за поиск в базе уже встречавшихся угроз, второй – выявляет новые опасности. В схеме от иммунной системы наследуется механизм подтверждения результатов. Он основывается на получении стимулирующего сигнала от соседних детектирующих наборов при анализе массива данных, предоставляемых одним и тем же субъектом (рис. 3).

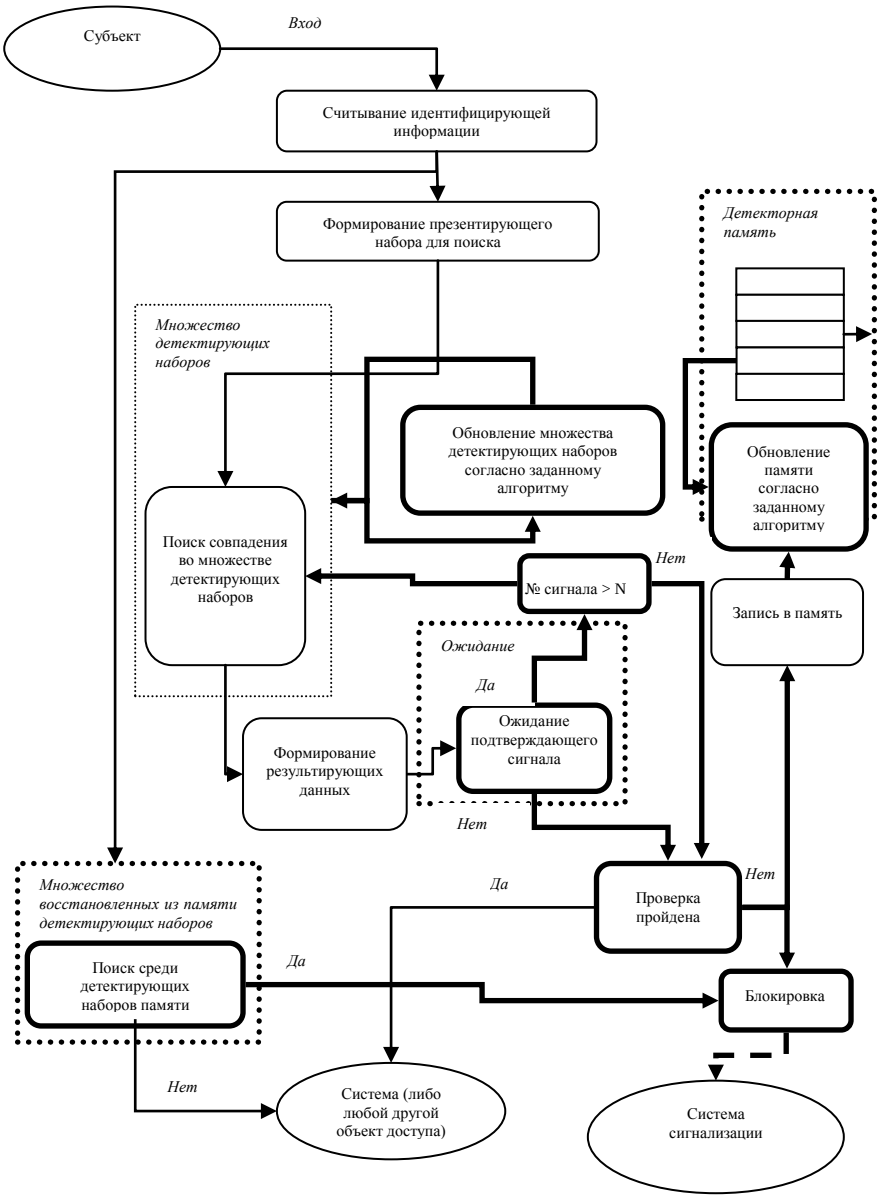

Рис. 3. Двухпотоковая аутентификация субъекта с использованием обновляемого множества детектирующих наборов

К перспективным моделям, использующим рассматриваемую аналогию, по мнению автора, относятся следующие:

– модель оценки эффективности СЗИ ИТ;
– модель диагностики СЗИ ИТ;
– модель выявления предпосылок действия угроз (модель «мертвого кода»);
– корпоративная модель СЗИ;
– модель прогнозирования действия угроз.

Реакции иммунной СЗИ ИТ лежат в основе контроля включаемых модификаций штатного ПО, запрета включения несовместимых модификаций.

Нарушения в работе СЗИ приводят к развитию развала штатной работы функционального ПО, нарушению отдельных функций СЗИ, к действию угроз в работе ПО на начальной стадии функционирования ПО, возникновению размножения зараженного ПО, преждевременному старению ПО и т.д.

Центральная задача иммунологии ИТ

С ростом числа и сложности современных ИТ и ТКС необходимо переосмыслить основополагающие моменты науки защиты информации. Существующее представление ее целей как необходимости поиска ответа на поступающие на отдельные рабочие места угрозы, причем уже после проявления атаки, не соответствует растущему полю угроз и темпам их действий. Рост сложности корпоративных сетей, включающих иногда десятки тысяч взаимосвязанных рабочих мест, причем с различными программно-техническими и функциональными конфигурациями компонент корпоративных сетей, попытки построения аналогичных систем СЗИ на каждом рабочем месте приводят к плачевным результатам. Отличия конфигурации и состава программно-аппаратных компонент рабочих мест в одной и той же корпоративной сети, работающей в условиях необходимого подключения к глобальным сетям и обменивающейся данными и программами с другими корпоративными сетями, приводят к необходимости построения СЗИ, индивидуально ориентированных на каждое рабочее место. СЗИ отдельных рабочих мест охватывают все уровни компонент, и, соответственно, ввиду отличий этих компонент становятся индивидуальными СЗИ на этих рабочих местах. СЗИ на каждом рабочем месте, охватывающая все функциональные компоненты, должна контролировать и различать санкционированный обмен информацией от воздействия угроз на всех уровнях компонент рабочих мест корпоративной сети.

В то же время сегодня нормативные документы по защите информации не делают различий в требованиях к отдельным рабочим местам и к крупным корпоративным сетям.

В заключение можно сказать, что конструктивное применение аналогии иммунных систем и СЗИ ИТ и ТКС с целью повышения уровня защищенности позволяет объективно оценить реальную защищенность как отдельных рабочих мест ИТ и ТКС, так и крупных корпоративных систем.

При создании крупных (более 10 тысяч рабочих мест) корпоративных сетей оценка необходимого уровня их защищенности в целом для обеспечения соответствующих классов защищенности на одиночных рабочих местах, входящих в корпоративную сеть, в тысячи раз превышает уровень требований, обозначенный в руководящих документах ФСТЭК России. Требования к моменту создания СЗИ ИТ и ТКС вообще не обозначены. В то же время в живых организмах иммунная система зарождается и строится параллельно, а иногда и раньше других функциональных систем. В случае традиционного построения СЗИ ИТ после формирования конфигурации аппаратных и программных функциональных средств ИТ потери от последующей переконфигурации или доработки средств СЗИ очень велики. Построение СЗИ во время создания ИТ позволяет избежать таких потерь и потерь от раннего действия угроз безопасности.

Построение ответных средств противодействия угрозе, поступившей на отдельное рабочее место в сети, также должно распространяться максимально быстро на все рабочие места сети (что оправдано экономически и технически), как в иммунной системе живых организмов. Пик создания и установки средств противодействия угрозе должен опережать пик распространения угрозы на другие рабочие станции сети.

Необходима также организация передачи ранее накопленных средств СЗИ, ориентированных на конкретные угрозы, на вновь конфигурируемые функциональные средства сети, то есть должно осуществляться наследование средств и методов защиты от угроз.

Приведенный краткий анализ целесообразности использования аналогии СЗИ ИТ и ТКС с иммунной системой живых организмов показывает необходимость ее дальнейшего изучения ввиду усложнения современных ИТ. Использование технологии и организации СЗИ ИТ с аналогичными иммунологическими методами позволяет сократить расходы и повысить эффективность СЗИ ИТ.

Литература

1. Нестерук Ф.Г., Суханов А.В. и др. Адаптивные средства обеспечения безопасности информационных систем. Проектирование и создание интеллектуальных средств защиты информации, адаптивных к изменению угроз; [под ред. Л.Г. Осовецкого]. СПб.: Изд-во Политехн. ун-та, 2008. 626 с.

2. Осовецкий Л.Г., Кравченко А.Ф. Иммунология ИТ. СПб: Изд-во ЛФЭИ, 2007. 70 с.

3. Немолочнов О.Ф., Твердый Л.В., Осовецкий Л.Г. Корпоративная теория информации. Изд-во СПб ГУ ИТМО, 2005. 87 с.

4. Липаев В.В. Методы обеспечения качества крупномасштабных программных средств. М.: СИНТЕГ, 2003. 520 с.