DOI: 10.18372/2410-7840.23.15431
УДК 004.056.53

АДАПТИВНЫЙ ПОДХОД К ПОСТРОЕНИЮ И ОБЕСПЕЧЕНИЮ ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Александр Архипов

Рассмотрено применение адаптивного подхода к построению и обеспечению функционировании эффективной системы защиты информации (СЗІ), создаваемой организацией-владельцем информационного ресурса в конфликтной ситуации «атака / защита», возникающей при реализации атакующей стороной угроз относительно защищаемого ресурса. Анализируется содержание основных концепций адаптивного управления системой защиты информации на различных стадиях развития информационных технологий, в частности, обеспечение адекватных трансформаций парадигмы защиты, обусловленных изменениями в стратегии и тактике действий атакующей стороны. Исследуются особенности и возможности практического применения новых концепций защиты, например, предполагающих несостоятельность требования по принятию мер для предотвращения возможного опасного инцидента в случае неоправданной дороговизны их осуществления в сравнении с оценкой риска потерь, возникающих в результате реализации инцидента. Предлагается применение подхода, суть которого состоит в использовании при создании и управлении СЗІ сведений об особенностях и характере поведения обеих сторон-участников конфликта. Обобщение и «упаковка» указанных сведений реализуется в форме математических моделей – рефлексивных рисков, структура и набор которых определяются выделенными типовыми сценариями развития ситуации «атака / защита». Анализ и исследование моделей дает оценочную информацию, позволяющую обеспечить эффективное и рациональное инвестирование в СЗІ организации, сбалансировав финансово-экономические возможности организации с ее требованиями и возможностями в сфере защиты информации.

Ключевые слова: *информационная система, система защиты, адаптация, приоритизация, угрозы, атаки, уязвимости, риски, риск-ориентированный подход, рефлексивная модель, парадигма защиты.*

ВСТУПЛЕНИЕ

Практически любая идеология построения системы защиты информации (СЗИ) содержит в себе элементы адаптивного подхода, суть которого – организация такого набора защитных сервисов (функций) СЗИ, который в состоянии предотвратить реализацию угроз относительно защищаемой информации.

Успешная СЗИ должна гарантировать полноту и своевременность адаптации функционала защиты к возможным внешним и внутренним угрозам, установление множества (перечня, списка) которых представляет собой нетривиальную проблему.

В своем развитии и осмыслении эта проблема порождает несколько вариантов реализации адаптации СЗИ. Хронологически первый из них, соответствующий раннему этапу развития современных информационных технологий, можно назвать ***естественной адаптацией*** [5].

Суть его в том, что на этом этапе для задач, связанных с получением, транспортировкой и обработкой информации, был характерен достаточно высокий уровень типизации и стандартизации предлагаемых решений, реализуемых на базе унифицированного программного и технического обеспечения, входящего в состав информационно-коммуникационных систем (ИКС).

Анализ инцидентов, фиксируемых в ходе эксплуатации ИКС, давал возможность выявить характерные уязвимости в их компонентах, позволявшие организовывать и проводить атаки, наносящие ущерб циркулирующей в ИКС информации. Исследование и обобщение способов предотвращения этих атак вело к построению устойчивых шаблонов типовых задач защиты для определенных категорий ИКС и соответствующих им совокупностей функциональных требований безопасности (профилей защиты). В СЗИ, реализующей адекватно выбранный профиль защиты, необходимо выполнялся принцип полного перекрытия угроз.

СУТЬ ПРОБЛЕМЫ

К сожалению, при современном уровне развития информационных технологий построение

СЗИ с учетом только ретроспективно найденных угроз является явно недостаточным. Постоянно нарастающая интенсификация темпов разработки, объемов и сфер применения информационных технологий ожидаемо сопровождается резким ростом уязвимостей ИКС и, следовательно, увеличением числа потенциально возможных атак, эксплуатирующих эти уязвимости.

Стремление к составление максимально полного перечня уязвимостей ИКС, фактически возведенное в норму положениями стандарта ISO/IEC 15408, требует проведения очень детального, кропотливого, длительного и трудоемкого анализа, результаты которого стимулируют постоянное расширение функционала защиты.

Попытка применения в этой ситуации системы защиты по схеме с полным перекрытием (назовем гипотетический вариант реализации подобной защиты ***асимптотической адаптацией*** [5]) влечет непомерно большие инвестиции в ее разработку и построение, что фактически исключает возможность учета неограниченно возрастающего объема сведений об уязвимостях и угрозах ИКС в формате построения реальной СЗИ [18].

Выходом в создавшейся ситуации является сокращении множества «всех возможных» угроз до группы так называемых актуальных угроз, являющихся наиболее опасными как для информационных ресурсов организации, так и для активов организации в целом. Выявление актуальных угроз опирается на результаты проведения процедуры приоритизации [10] угроз – их ранжирования (упорядочивания) согласно определенному показателю или системе показателей, в качестве которых в стандартах серии ISO/IEC 27XX, в частности, в стандарте ISO/IEC 2705, рекомендуется использовать риски информационной безопасности.

Назовем ***риск-ориентированной адаптацией*** процесс формирования структуры и состава СЗИ, базирующийся на выделении группы актуальных угроз, являющихся для организации основным источником возникновения наиболее значимых информационных рисков. **Целью данной статьи** является рассмотрение основных аспектов и перспектив использования принципа адаптации (и в первую очередь риск-ориентированной адаптации) для построения и функционирования СЗИ.

Риск-ориентированная адаптация, содержательная часть.

В основе риск-ориентированной адаптации лежит последовательное решение двух задач:

- выявление угроз безопасности информации, актуальных для данной конкретной организации с учетом ее целей и специфики функционирования;

- построение СЗИ на базе изучении и анализе источников формирования и свойств актуальных угроз.

Содержание первой задачи – выделение группы актуальных угроз (иногда используются семантически близкие термины: «значимые» или «существенные» угрозы) – состоит в ранжировании (упорядочивании) угроз информации по степени опасности, которую они представляют для организации, что реализуется путем проведения анализа и сопоставление угроз между собой по степени выраженности у них специфичных свойств, называемых опасными факторами [2]. Собственно, процедура сопоставления и ранжирования угроз называется приоритизацией угроз [10], менее употребляемый термин – «фильтрация» угроз [6].

В зависимости от глубины и детализации выполняемого анализа для описания угрозы может привлекаться различное число факторов, т.е. проведение сопоставительного анализа угроз для сравнения и ранжирования их степени опасности опирается на векторные характеристики угроз, причем размерность векторов у разных угроз может быть разной, что усложняет проведение приоритизации.

Например, в [6] для отнесения угроз к актуальным предполагается анализ следующих факторов:

- величина потерь (урона), наносимых организации в случае успешной реализации угрозы;

- наличие уязвимостей в ИКС, допускающих возможность реализации угрозы;

- вероятность успешного осуществления атак, использующих выявленные уязвимости.

При количественном задании значений потерь и вероятностей, следуя упомянутым выше рекомендациям стандартов серии ISO/IEC 27XX по интенсивному привлечению в практику менеджмента безопасности информации риск-ориентированного подхода, удается достаточно просто, рассчитав риски атак, свести векторное описание к скалярному, и далее, агрегировав риски атак в риски угроз, упорядочить угрозы по убыванию величины их рисков. К сожалению, единая общепринятая схема проведения приоритизации угроз отсутствует, описываются различные варианты приоритизации: уязвимостей, рисков и угроз, однако фактически все они - элементы одной общей схемы приоритизации.

Исходным пунктом этой схемы является составление максимально полного «стартового» перечня уязвимостей ИКС. Эксплуатация отдельной уязвимости или их набора («цепочки» уязвимостей) позволяет реализовать атаку, эффективность которой характеризуется уровнем значения частного риска, возникающего в результате нарушения этой атакой нормального режима работы организации. Критерием недостаточной эффективности атаки является пренебрежимо малый уровень порождаемого ею частного риска, что служит основанием для исключения уязвимости, определяющей возможность возникновения этой атаки, из «стартового» перечня уязвимостей. Одновременно формируется список актуальных угроз, в который вносятся угрозы, реализуемые одной эффективной атакой либо их совокупностью при условии, что интегральный (обобщенный) риск анализируемой угрозы оказался выше некоторого минимального порогового уровня. Рассмотрим более детально отдельные аспекты приоритизации на иллюстративном примере. Предположим, что среди обнаруженных в ходе обследования ИКС уязвимостей выявлена группа уязвимостей $\{V=\{v_j\}\}$, $j=\overline{1,k}$, любая из которых позволяет провести эффективную атаку, цель которой – попытка осуществления угрозы t. Опасность произвольной атаки α_j характеризуется ее частным риском

$$\rho_j = p_{aj} q_{\alpha j}, \qquad (1)$$

где p_{aj} - вероятность успешной реализации атаки, $q_{\alpha j}$ - потери, понесенные при этом организацией. Если атаки независимы и несовместны, опасность угрозы t в целом характеризуется интегральным риском R, рассчитанном на полной группе событий, включающей k опасных событий (множество атак $A=\{\alpha_j\}$, $j=\overline{1,k}$) и одно $(k+1)$-ое событие, которому соответствует режим безопасного функционирования ИКС (отсутствие каких-либо атак/угроз) с параметрами: $q_{\alpha,k+1}=0$, $p_{a,k+1}=1-(p_{\alpha 1}+...+p_{\alpha k})$.

В этой ситуации расчет интегрального риска R осуществляется с применением формулы суммарного риска R_Σ [2], [1], [18] агрегирующей риски отдельных атак:

$$R = R_\Sigma = \sum_{j=1}^{k} \rho_j = \sum_{j=1}^{k} p_{aj} q_{\alpha j}. \qquad (2)$$

В общем случае при вычислении интегрального риска R возникает проблема методологического плана, характерная для случая, когда угроза реализуется путем проведения нескольких так называемых одновременных (совместных) атак (simultaneous attacks [18]).

Осуществление одновременных атак ведет к увеличению вероятности реализации анализируемой угрозы и, как следствие, к росту уровня привносимого ею интегрального риска, вычисление которого сопряжено с определенными трудностями. Для более адекватного понимания проблемы несколько изменим формулировки приведенного выше примера: отменим требование несовместности атак и будем полагать, что успешное завершение любой из атак приводит к одинаковым потерям q.

Если и в этом случае для расчета интегрального риска R угрозы t применить формулу суммарного риска, получаем:

$$R = R_\Sigma = \sum_{j=1}^{k} \rho_j = \sum_{j=1}^{k} p_{aj} q = q \sum_{j=1}^{k} p_{aj}. \qquad (3)$$

С другой стороны, если известна вероятность p_t реализации угрозы t, риск угрозы t рассчитывается по формуле $R = qp_t$.

Сравнивая эту формулу с выражением(3), получаем равенство $p_t = \sum_{j=1}^{k} p_{a_j}$, при этом для вероятности p_t, как и любой другой вероятности, должно выпляться требование $0 \le p_t \le 1$.

Однако правое неравенство этого требования для атак, вероятности реализации которых удовлетворяют условию $1/k < p_{aj} \le 1,\ j = \overline{1,k}$, очевидно не выполняется: $p_t = \sum_{j=1}^{k} p_{a_j} > 1$.

Следовательно в самом общем случае формула (3) не верна, а рассчитанное по ней значение риска R может оказаться завышенным. Причиной возникновения такой ситуации является неприменимость формулы суммарного риска для расчета интегрального риска угрозы при наличии совместных атак.

Методически корректный способ расчета оценки интегрального риска в этой ситуации описан в [1], а особенности его практического выполнения – в [2].

К сожалению, сам расчет требует проведения довольно трудоемких и громоздких вычислений, в свою очередь основывающихся на значительных объемах количественной информации.

На практике реализовать все это весьма сложно, поэтому в руководящих документах самого разного уровня (стандартах, отраслевых, ведомственных, корпоративных наставлениях, рекомендациях и т.п.) акцент делается на изложении методик и положений, работающих с данными в качественной форме представления.

Построение СЗИ на базе изучении и анализе источников формирования и свойств актуальных угроз. После выделения группы актуальных угроз, благодаря проводимому в ходе этого этапа детальному анализу механизмов реализации атак и угроз, появляется возможность наилучшим образом выбрать методы и средства защиты, реально соответствующие уровню гарантий защиты, сформировать прототип СЗИ, который будет исследоваться, дорабатываться и модифицироваться уже непосредственно в ходе решения задачи риск-ориентированной адаптации построения СЗИ. Это позволит объективно оценивать инвестиционные бюджеты на создание того или иного варианта СЗИ, сопоставлять их с общим бюджетом организации и т.п.

Задача построения СЗИ в последних редакциях стандартов серии ISO/IEC 27XX, в частности, стандарта *ISO/IEC 2705:2018 — IИнформационные технологии — Методы безопасности — Управление рисками информационной безопасности*, позиционируется как одна из задач, составляющих основное содержание управления (менеджмента) безопасностью информации. Решение этой задачи, гармонизированное с требованиями базового управленческого стандарта *ISO 9001:2015 - Системы менеджмента качества – Требования*, основывается на применении риск-ориентированного подхода, гарантирующего результативность построения и функционирования систем менеджмента в любых сферах деятельности.

В общем случае результативность (качество) функционирования СЗИ определяется ее соответствием набору требований безопасности, т.е. векторным показателем (критерием), что существенно усложняет решение задачи управления качеством.

Обычный выход в этой ситуации – уменьшение размерности векторного критерия, в идеальном случае - агрегирование (свертывание) векторного критерия в обобщенный скалярный, достижение экстремального значения которого свидетельствует об оптимальном управлении процессом функционирования СЗИ.

Форма и структура введенного показателя качества функционирования СЗИ должны обеспечивать его универсальность, в частности, возможность его применение для сопоставления различных вариантов СЗИ как на этапе проектирования, так и для оценки качества уже работающих систем защиты.

Указанным свойствам критерия качества СЗИ в полной мере удовлетворяет риск как показатель возможных потерь организации, возникающих в силу существования определенных обстоятель-

ств. В частности, невыполнение требований к СЗИ приводит к возникновению ряда информационных рисков, которые, благодаря представлению их в единой количественной (например, денежной) шкале, агрегируются в интегральную (обобщенную) оценку качества функционирования СЗИ.

Ее нулевому значению соответствует случай удовлетворения всех требований к режиму безопасного функционирования СЗИ, наибольшему риску - диаметрально противоположная ситуация.

Поэтому следующим шагом риск-ориентированной адаптации после выполнения приоритизации, выделения и анализа совокупности актуальных угроз $T_a = \{t_i\}$, $i = \overline{1,n}$, является нахождение ***агрегированного (обобщенного) информационного риска организации*** путем объединения (агрегирования) отдельных (частных) интегральных рисков актуальных угроз в одном общем рисковом показателе.

В ряде случаев процедура агрегирования может оказаться достаточно простой. Например, при условии независимости и несовместности актуальных угроз, а также независимости наступивших в результате их реализации последствий, агрегированному (обобщенному) интегральному риску организации будет соответствовать суммарный риск

$$R_s = \sum_{i=1}^{n} R_i , \qquad (4)$$

где R_i, $i = \overline{1,n}$ - интегральный риск каждой отдельной угрозы из выделенной группы актуальных.

К сожалению, для организаций с достаточно сложной структурой, располагающих значительным объемом информационных ресурсов (ИР) и интенсивно использующих в своей работе комплексные информационные технологии, вычисление агрегированного интегрального риска организации R_s в условиях возможного воздействия нескольких угроз, допускающих совместную реализацию с проявлением взаимосвязанных и взаимозависимых последствий, представляет нетривиальную задачу [1, 2].

Пример решения подобной задачи приведен в [2].

Набор данных, включающих агрегированный интегральный риск R_s совместно с совокупностью рисков актуальных угроз R_i, $i = \overline{1,n}$, представляет собой $(n+1)$-мерный вектор, количественно описывающий ситуацию с безопасностью (защищенностью) информации в организации при отсутствии в ней СЗИ.

Приняв его за некоторую исходную точку (координату) в пространстве состояний безопасности организации, получаем возможность визуально сопоставить риски исходного состояния безопасности с рисками организации после включения в ее состав СЗИ, описав эту новую ситуацию $(n+1)$-вектором остаточных рисков R_{so}, R_{io}, $i = \overline{1,n}$.

Учитывая, что фактором, весьма существенно влияющим на уровень защищенности информации является объем инвестиций c в СЗИ, для оценивания эффективности осуществления защитных мер и эффективности функционирования СЗИ в целом обычно используется показатель вида [3], [4]:

$$\Delta_s(c) = \frac{\Delta R_s(c)}{c} = \frac{R_s - R_{s0}(c)}{c}, \qquad (5)$$

где $\Delta R_s(c)$ – уменьшение значения исходного риска, обусловленное введением СЗИ (так называемая «экономия риска»), в общем случае зависящее от объема инвестиций c. Очевидно, что согласно формуле (5) лучшее решение проблемы защиты информации в организации обеспечит тот вариант СЗИ, для которого показатель (5) примет наибольшее из всех своих возможных значений (наилучшее соотношение «качество/стоимость»).

Поскольку результаты оценивания рисков влияют на объем средств, инвестируемых в СЗИ, формирование понятного и прозрачного процесса анализа информационных рисков является важнейшим условием успешного функционирования системы менеджмента безопасности информации (СМБИ) организации.

Этим же объясняются жесткие требования к объективности и точности рассчитываемых оценок рисков. Применение в подобных условиях суммарного риска в качестве оценки интегрального риска обычно дает существенно завышенное оценочное значение, способствуя необоснованному увеличению объема инвестиций в построение СЗИ. Кроме того, при расчете рисков используются, как правило, экспертные оценки, что вносит в расчетные значения субъективные погрешности, снижающие надежность результатов всего анализа в целом. К сожалению, ныне действующие стандарты управления СМБИ не содержат предписаний по решению задачи оптимизации структуры и параметров СЗИ, предлагая лишь весьма общую схему управления информационными рисками (например, стандарт ISO/IEC 27005), позволяющую осуществлять перебор вариантов СЗИ. Эта схема реализуется в форме итеративной процедуры, предназначенной для достижения следующих целей:

- согласование и увязка требований к уровню и параметрам рисков с методами и средствами уменьшения и нейтрализации рисков, что составляет суть задачи обеспечения собственно безопасности информации;

- разумная балансировка объема инвестиций в СЗИ по отношению к уровню возможных потерь организации, обусловленных реализациею угроз информации.

Запуск очередной итерации (второй, третьей, … и т.д.) осуществляется в случае необходимости получения дополнительной информации для составления перечня актуальных угроз и формирования профиля защиты, а также при невозможности построения СЗИ с учетом соблюдения уровня заданных функциональных требований безопасности, оставаясь при этом в пределах объема инвестиций, разрешенного бюджетом организации.

В последнем случае проведению очередной итерации предшествует пересмотр допустимых (предельных) значений показателей, используемых в процессе анализа и обработки частных рисков атак и интегральных рисков угроз так, чтобы выполнялось одно из базовых требование стандарта ISO/IEC 27005 (разд. 4.3): объем выделенных инвестиций не должен превышать агрегированного интегрального риска организации. В обоих случаях в ходе итераций должна происходить адаптация принимаемых при создании СЗИ решений к реальному контексту функционирования организации.

Поэтому для успешной реализации итеративной процедуры риск-ориентированной адаптации необходимо упорядочить рассмотрение вариантов СЗИ, организовав их целенаправленный перебор, обеспечивающий на очередной k-ой итерации значение показателя $\Delta_s^{(k)}(c) \geq \Delta_s^{(k-1)}(c)$.

Гипотетически при $k \to \infty$ целенаправленный перебор бесконечно большого числа вариантов должен привести к оптимальному решению, однако для конечного значения k реально получение лишь некоторого квазиоптимального реультата.

Введение итераций позволяет обеспечить поиск и получение дополнительной информации для осуществления более глубокой и целенаправленной адаптации, однако необходимость повторной обработки в каждом очередном цикле итераций нового расширенного объема информации крайне затягивает и усложняет и без того громоздкую процедуру адаптации.

В целом применение для формирования структуры и состава СЗИ риск-ориентированного подхода, суть которого – анализ исходного обширного множества подлежащих «перекрытию» потенциально возможных угроз для сокращение его до компактной группы так называемых актуальных угроз, на первый взгляд выглядит достаточно убедительно.

Однако сама процедура выделения актуальных угроз для своего запуска и реализации требует наличия «стартового», первоначально максимально полного перечня всех возможных уязвимостей / атак, составление которого является весьма кропотливым, длительным, трудоемким и при этом весьма субъективным. Селекция эффективных атак, осуществляемая в первую очередь под прессом доминирующего стремления не

пропустить в ходе анализа элементов «стартового» перечня опасную атаку, ведет к получению излишне расширенного перечня актуальных угроз и в конечном итоге – к необоснованному росту объема инвестиций в СЗИ [3, 5]. По-видимому, практика подобного экстенсивного роста инвестиций может быть прервана введением некоторого предельного уровня их объема.

Особо актуальным в сложившейся ситуации представляется требование объективного (доказательного?) задания предельного объема этих инвестиций. Необходимость решения данной проблемы стимулирует попытки применения более глобализированного подхода к рассмотрению организации и ее рисков, в рамках которого технологические аспекты оценивания рисков, в частности, наиболее громоздкий и трудозатратный детальный анализ угроз и уязвимостей ИКС, практически не используется. Вместо этого акцентированное внимание уделяется составлению и анализу моделей развития сценариев информационных рисков, формализации зависимости бизнеса организации и совокупной ценности ее основных активов от уровня безопасности и состояния информационных активов. В частности, в статье [16] предпринята попытка нахождения в самой общей постановке оценки оптимального объема инвестиций, необходимого для обеспечения безопасности информации. К сожалению, изложенные в этой работе результаты, базирующиеся на введении совокупности формальных требований к описанию ситуации «атака/защита» (модель Гордона-Лоэба), практически исключают возможность своей привязки к особенностям и свойствам конкретной реальной организации, к целям и задачам обеспечивающей ее деятельность ИКС, к функциям и параметрам создаваемой СЗИ.

Построение СЗИ с целевой адаптацией к потенциалам атакующей и защищающейся стороны. Рассмотрим подробнее конфликтную ситуацию (далее именуемую ситуацией «атака/защита»), складывающуюся при возможной реализации стороной **A** угрозы t относительно информационного ресурса I, владелец которого – сторона (организация) **B** [4, 5] (сам конфликт возникнет с началом активных действий). Очевидно, что проявить активность, стать инициатором конфликта может только сторона **A** (далее – атакующая сторона), под которой будем понимать любую сущность (хакер, вредоносный код, внутренний злоумышленник и т.п.), злонамеренные действия которой направлены на информацию, циркулирующую в ИКС организации, сказываясь, в случае успешной реализации, на состоянии и стоимости активов всей организации **B** (защищающаяся сторона) в целом. Особенности развития конфликта, его итоги зависят в первую очередь от соотношения потенциалов участников конфликта.

Под ***потенциалом атакующей стороны*** обычно [3] понимается комплекс следующих факторов: компетентность и уровень мотивации атакующего (при антропогенном характере атаки), ресурсное обеспечение (в том числе финансово-экономическое), способствующее успешному осуществлению атакующих действий. Возможность учета названых факторов рассмотрена в [4], где, в зависимости от наличия и выраженности этих факторов, вербально описаны модели типовых сценариев поведения атакующей стороны для набора типовых ролей, формирующих специфическую ролевую структуру (классификацию):

1. ***Скрипт кидди*** – как правило, одиночка, не имеющий существенной подготовки, знаний и опыта, использующий для атаки скрипты или программы, разработанные другими, не понимающий механизма их действия, неспособный к креативу, самостоятельным эффективным атакующим решениям, с достаточно скромными ресурсными возможностями; обычно его не волнуют политические или финансовые соображения, точнее финансовый интерес не составляет единственную и определяющую мотивацию его действий, т.к. представление о рыночной стоимости атакуемого ресурса обычно просто отсутствует. Чаще всего цель скрипт кидди – произвести впечатление на свое окружение, завоевать авторитет среди коллег-представителей своей компьютерной субкультуры, стремление породить хаос, отказ либо нарушение сервисов, наконец, просто

«спортивный интерес» [15]. По оценке А.В.Лукацкого [7], скрипт кидди составляют до 95% от общего числа злоумышленников, атакующих информационные и компьютерные системы, т.е. это наиболее распространенный тип нарушителя, необходимость защиты от которого является первоочередной задачей, решаемой при построении СЗИ. Следует заметить, что «под крышу» скрипт кидди можно подвести различные вредоносные коды (вирусы, черви, пр.).

2. ***Самозанятый профессионал***, работающий один либо в составе группы прфессионалов, обладающий необходимыми знаниями, навыками и достаточным опытом, прекрасно разбирающийся в технологии атак, с глубоким пониманием методов взлома систем защиты, для которого хакинг – основная деятельность, носящая очевидный коммерческий характер, цель которой - финансово-экономическая выгода.

3. ***Профессионал-исполнитель*** - хакер, по своим объективным характеристикам и возможностям соответствующий перечисленному выше в п.2, но выполняющий задания в интересах силовых структур или спецслужб как наемный исполнитель, действующий в рамках определенных взаимодоговорных отношений.

4. ***Хактивист*** - идейный хакер («кибератвист»), использующий киберпространство в целях продвижение политических либо социальный идей (задач), организующий в киберпространстве акции гражданского «электронного» неповиновения, старающийся привлечь внимание власти и общественности (иногда в довольно жесткой форме) к тем или иным вопросам и проблемам современного общества путем синтеза социальной активности и хакерства.

Отметим, что для трех первых элементов (ролей) приведенной классификации основным дифференцирующим признаком является уровень компетентности атакующей стороны (т.е. наличие знаний, умений и опыта практической деятельности), интенсивно наростающий в направлении ***скрипт кидди→самозанятый профессионал→профессионал-исполнитель***.

Базовой характеристикой хактивиста, отличающей его от трех предыдущих ролей, является наличие у него определенных идеологических и морально-этических установок. Очевидно, что успешность действий атакующей стороны, как и окончательный сценарий развития и завершения конфликта в значительной мере зависят и от ***потенциала защиты***. Последний определяется главным образом объемом инвестиций c в СЗИ, уровнем s информационной зрелости [10] защищающейся стороны, а также интегральной характеристикой важности защищаемых информационных ресурсов, которая часто определяется стоимостью или ценностью информационных ресурсов организации. Далее в качестве этой интегральной характеристики будем использовать q – полные (максимальные) потери защищающейся стороны в случае успешного завершения направленных против нее атакующих действий.

В статье [3] приведенному выше набору типовых ролей, каждой из которых отвечает свой модельный сценарий поведения атакующей стороны, поставлены в соответствие математические модели агрегированных интегральных рисков, определяющих возможные потери защищающейся стороны в случае реализации того или иного ролевого сценария. Эти модели рисков отражают особенности каждой из введенных выше типовых ролей, в связи с чем они получили название ***моделей рефлексивных рисков*** (от лат. reflexus – отображение, отражение). Фактически введение рефлексивных рисков свидетельствует о возможном наличии серьезных расхождений в способах анализа рисков как для различных типовых ролей атакующего, так и для различных ситуаций «атака/защита», приводящих в конечном итоге к отличиям в получаемых математических моделях агрегированных интегральных рисков. Это свидетельствует о необходимости целевой адаптации риск-ориентированного подхода при его использовании для анализа конкретной ситуаций «атака/защита». Ниже рассмотрим несколько моделей рефлексивных рисков и их применение для получения полезных (но не оптимальных) решений, используемых для построения СЗИ. ***Модель рефлексивного риска для первой типовой роли*** – скрипт кидди,

представляет собой агрегированный интегральный риск организации, задаваемый выражением

$$R(c) = P_t P_v q = P_t \frac{q}{q + sc} q, \qquad (6)$$

где P_t - вероятность активации в данное время и в данном месте угрозы t информационным ресурсам организации (аналог статистических оценок, определяемых американским институтом стандартов NIST), P_v – вероятность успешной реализации активированной угрозы. При отсутствии сведений о количественном значении P_t, ввиду широкой распространенности угрозы со стороны скрипт кидди, в первом приближении можно полагать $P_t = 1$.

Подобное предположение хорошо подтверждается характеристикой поведения скрипт кидди, данной В. Столлингсом [11]: «тупое желание бесконечно долго «стучаться в закрытые двери», проверяя все уязвимости системы».

Эта же цитата в какой-то степени содержит пояснение к непосредственно следующей из выражения (6) формуле

$$P_v = \frac{q}{q + sc}, \qquad (7)$$

согласно которой вероятность P_v зависит только от мер по обеспечению безопасности информации, принимаемых защищающейся стороной **B** (эффективность и полнота мер определяется объемом инвестиций c в СЗИ и уровнем s информационной зрелости организации).

Односторонняя зависимость вероятности P_v лишь от принятых защитных мер согласуется с упоминавшейся особенностью поведения скрипт кидди, состоящей в отсутствии новизны в предпринимаемых ими атакующих действиях.

В такой ситуации СЗИ, реализующая принцип полного перекрытия «старых» угроз и их очевидных модификаций, достаточно надежна.

Степень защищенности организации возрастает с увеличением объема инвестиций c при условии их грамотного использования, т.е. с ростом s. Анализ рефлексивного риска (6), его сопоставление с размером инвестиций в СЗИ и «экономией риска» в формуде (5) позволяет получить формулу для опредения эффективного объема инвестиций [4]:

$$c_{eff}(s) = arg \max_{c \in C}(R(c) - R(0) - c)) =$$

$$arg \min_{c \in C}(R(c) + c)) = \frac{q}{s}(\sqrt{P_t s} - 1) \qquad , \qquad (8)$$

где C – множество значений c, представляющих «разумные» инвестиции (для которых «экономия риска» $\Delta_R(c) = R(c) - R(0) > c$), сосредоточенные в диапазон $0 \le c \le q(s-1)/s$, а также формулы для расчета значения вероятности P_v и риска R в условиях эффективного инвестирования [2]:

$$P_v(c_{eff}) = \frac{1}{\sqrt{P_t s}}, \quad R(c_{eff}) = P_v(c_{eff}) P_t q = q\sqrt{\frac{P_t}{s}}. \qquad (9)$$

В пределах диапазона «разумных» инвестиций зависимость значений эффективного объема инвестиций c_{eff} от параметра s носит одноэкстремальный характер с максимумом, равным [3]:

$$\max[c_{eff}(s)] = 0{,}25 q P_t. \qquad (10)$$

При $P_t = 1$ величина эффективных инвестиций в СЗИ окажется наибольшей, т.е. значение максимального объема инвестиций в СЗИ составит $c_{eff\max} = 0{,}25q$ или 25% стоимости ресурса q, который является объектом защиты, однако для продуктивных защитных решений (например, при $s = 60$) в соответствии с формулой (8) даже при $P_t = 1$ объем инвестиций в СЗИ может оказаться на уровне 11-13% от стоимости защищаемого ресурса.

Полученные результаты хорошо согласуется с эмпирическими оценками объема инвестиций, приведенными в ряде публикаций [2, 6, 9], авторы которых акцентируют внимание на сумме в 15-20 % от стоимости активов ИС.

Таким образом, результаты, полученные в ходе исследования модели рефлексивного риска (6), позволяют в реальной ситуации, зная значения параметров q, s, найти оценки показателей c_{eff}, $c_{eff\max}$, $R_{in}(c_{eff})$ и задаться величиной при-

емлемого для данной организации «разумного» объема c инвестиций в СЗИ [2], [3]. Рассматривая его как ресурсное ограничение, далее можно приступать к решению задачи распределения выделенных инвестиций на ограниченном множестве возможных функций и механизмов защиты, формируя на них структуру СЗИ из условия минимизации остаточного риска организации, сопоставления и анализа количественных оценок показателей c_{eff}, q, $c_{eff\max}$, $R(c_{eff})$, $R(s,c)$ для различных значений параметра c, балансируя при этом финансово-экономические возможности организации с ее требованиями и возможностями в сфере безопасности информации.

Модель рефлексивного риска для второй типовой роли задается [2] выражением

$$R(c) = P_t P_v q = (1-\frac{D}{g})\frac{q}{q+s\frac{c^2}{D}}q, \qquad (11)$$

где g - ценность (важность) ресурса для атакующей стороны, D - ее обобщенные затраты на подготовку и реализацию атакующих действий, приведенные к денежной форме представления. Появление в модели риска новых параметров g и D, характеризующих интересы и мотивы поведения атакующей стороны, обусловлено адаптацией модели риска к новой типовой роли, для которой характерно значительное влияния возможностей атакующего на исход конфликта. В частности, первый сомножитель в правой части выражения (11), представляющий собой оценку вероятности P_t активации угрозы t

$$P_t = \frac{g-D}{g} = 1-\frac{D}{g} \qquad (12)$$

допускает следущую логико-эвристическую интерпретацию: чем выше чистая прибыль $g-D$, получаемая атакующей стороной в случае успешной реализации угрозы, тем выше мотивация атаки. По сути вероятность P_t в формуле (12) – это прибыль, отнесенная к ценности ресурса I, т.е. показатель эффективности предполагаемой атаки: чем больше g, тем ближе к 1 вероятность P_t; с уменьшением g, в случае $g \le D$, проведение атаки теряет смысл (если мотивация атакующего ограничивается рамками коммерческого интереса).

На практике это означает, что вероятность применения высокозатратных атак профессионалом, ориентированным на получение чисто коммерческой выгоды, крайне низка. Наконец, при $g >> D$ вероятность P_t практически равна 1, имеет место так называемаяя «целенаправленная (целевая) атака», характерной особенностью которой является наличие определенной конкретной цели – объекта атаки (организации, ведомства, физического лица), относительно которого осуществляются активные атакующие действия.

Влияние атакующей стороны проявляется и в модификации структуры эвристики, применяемой для вычисления оценки вероятности P_v: в знаменатель выражения (7) вводится мультипликатор $k = c/D$, позволяющий соотнести объемы, инвестируемые сторонами в защиту и атаку. В итоге для P_v получаем новую эвристику, используемую в формуле (11):

$$P_v = \frac{q}{q+skc} = \frac{q}{q+sc^2/D}. \qquad (13)$$

Диапазон разумных инвестиций, соответствующий модели (11), задается неравенством [3]:

$$\frac{qP_t}{2}(1-\sqrt{1-\frac{4D}{sqP_t^2}}) \le c \le \frac{qP_t}{2}(1+\sqrt{1-\frac{4D}{sqP_t^2}}). \qquad (14)$$

К сожалению, непосредственное нахождение для этой модели величины c_{eff} эффективного объема инвестирования аналитическим путем (используя соотношение (8)), как это было сделано для риска (6), оказывается невозможным.

Оценочное значение можно рассчитать, используя следующий прием. Введем переменную $z = sk$. Тогда модель (11) представима в виде

$$R(c) = P_t P_v q = P_t \frac{q}{q+zc} q, \qquad (15)$$

позволяющем для заданных значений q, s, k рассчитать по формуле (8), полагая $P_t = 1$, значение c_{eff}^*, затем $D = c_{eff}^*/k$. Задавая L раз новые

тройки q, s, k, заполним «таблицу эксперимента» $[q_j, s_j, k_j, c^*_{eff,j}, D_j]$, $j = \overline{1,L}$., по данным которой построим аппроксимирующую зависимость $\tilde{c}^*_{eff} = \mu(q,s,D)$.

Теперь для тройки значений q, s, D, характеризующих реальную ситувцию «атака/защита», можно будет рассчитать оценочное значение $\tilde{c}^*_{eff}$, соответствующее разумному объему инвестиций в каждом конкретном случае.

Следует отметить наличие ряда модификаций модели (11), обусловленных стремлением к обеспечению более глубокой адаптации этой модели рефлексивного риска к той или иной особенности ситуации «атака/защита».

Например, в [2] для оценивания вероятности P_t активации угрозы t предлагается формула:

$$P_t = 1 - \frac{D}{\gamma g}, \qquad (16)$$

где γ - дополнительный параметр, учитывающий «индивидуальные» особенности атакующей стороны: азарт, авантюризм, чрезмерную самоуверенность ($\gamma > 1$) или, напротив, излишнюю осторожность, нерешительность, неуверенность в себе и в своих силах ($D/g < \gamma < 1$). Несколько в иной постановке эта проблема рассмотрена в [4]. Коммерческие интересы, принцип экономической целесообразности и прагматизма не исчерпывают возможные мотивы, которыми руководствуется атакующая сторона в своих действиях.

В частности, побуждением к действию для атакующаей стороны может оказаться желание мести, наказания, асоциальные и иные устремления, конечным результатом которых станет намерение нанесения защищающейся стороне возможно большего ущерба (финансового, политического, имиджевого, морального и т.п.).

В этом случае вероятность активации P_t может задаваться формулой:

$$P_t = 1 - \frac{D}{q}, \qquad (17)$$

в соответствие с которой максимизация вероятности P_t происходит при неограниченном росте ущерба q, возникающем в результате реализации угроз информации. Эта ситуация демонстрирует возможность трансформации модели риска (11) самозанятого профессионала (путем ее фрагментарной модификации, детализации или упрощения) в другие модели, соответствующие иным сценариям поведения атакующей стороны.

Профессионал-исполнитель. В частности, примером обстоятельств, при которых принцип экономической целесообразности для атакующей стороны оказывается несущественным, является выполнение особо важного задания сотрудниками спецслужбы - профессионалами, подготовленными к осуществлению атакующих действий в киберпространстве [2, 3].

В этом случае задание атакующей стороны **A** – практическая реализация некоторой угрозы относительно ресурса I, - должна быть выполнена в любой ситуации, т.е. с вероятностью $P_t = 1$, что отличает данную типовую роль от предыдущей, в которой атакующая сторона в своих действиях исходит исключительно из положений экономического прагматизма.

В связи с особой важностью поставленной задачи, при ее решении снимаются обычно существующие ограничения. В частности, исполнитель может рассчитывать на привлечение для поддержки своих действий различных дополнительных ресурсов - финансовых, аналитических, технических, оперативных и т.п.: «если когда-нибудь разведывательное управление заинтересуется вашей компанией, приготовтесь к тому, что против вас будут направлены огромные людские и технические ресурсы (опытные технари, новейшее аппаратное обеспечение и прфессиональные шпионы)» [8].

Такая постановка вопроса позволяет обеспечивать осуществление чрезвычайно высокозатратных атак ($D \to \infty$).

Рефлексивная модель риска для этого случая проста:

$$R(c) = P_v q = \frac{q}{q + s\dfrac{c^2}{D}}\, q. \qquad (18)$$

Из нее очевидно, что со снятием ресурсных ограничений ($D \to \infty$) вероятность $P_v \to 1$, т. е. в

этой ситуации, если защищающаяся сторона, создавая свою СЗИ, опирается на принцип разумной достаточности, исходя исключительно из собственного («внутреннего») понимания существования конечной ценности q защищаемого ресурса I, успешная реализация угрозы атакующей стороной оказывается практически гарантированной, в итоге $R(c) \to q$.

1. Какие атаки и угрозы приводят к рефлексивным рискам (11), (18)? Для самозанятого профессионал характерен очень широкий спектр атак, начиная от массовых (DDOS атаки, фишинг, вирусы-шифровальщики и т.п.), атак социальной инженерии и заканчивая индивидуальными целенаправленными атаками, для профессионала-исполнителя – все ранее перечисленное плюс атаки класса APT (Advanced Persistent Threat, распространенные варианты перевода: комплексная таргетированная угроза [12], сложная протяженная (постоянная) угроза [13], сложная, развитая и устойчивая атака, направленная на захват контроля над целевой инфраструктурой [9]).

Основные этапы развития парадигмы защиты инфомации. Для выяснения фактической роли и сути адаптации в формировании СЗИ целесообразно бегло рассмотреть ретроспективу развития деструктивних действий в киберпространстве. В качестве начальной точки возьмем атаку сети ARPANET червем Морриса, которая на тот момент (ноябрь 1988 года) по сложности и своим последствиям, в частности, величине ущерба, оцененного в сумму от 98 млн. до 300 млн. долларов, может вполне соответствовать нынешнему классу APT угроз.

Реакцией на нее в сфере информационной безопасности явилось создание при университетах Беркли и Карнеги-Меллон (США) компьютерной группы реагирования на чрезвычайные ситуации - CERT (аббревиатура от Computer Emergency Response Team). В коонце 1980-х – первой половине 1990-х годов значительную часть инцидентов компьютерной безопасности составляли результаты проведения единичных целевых атак, организованных по конкретному заказу, и аналитические наработки экспертов CERT, занимающихся сбором информации об инцидентах, их классификацией и нейтрализацией, способствовали сохранению достаточно стабильного и высокого уровня кибербезопасности. Однако атакующая сторона, анализируя и осмысливая результаты единичных атак, начала повторять (тиражировать) успешные решения. В итоге многие атаки стали массовыми, не нацеленными на определенный объект, например, банк или конкретного клиента.

В этот период для криминального рынка оказалось выгоднее разрабатывать и реализовывать не уникальные, а именно массовые атакующие акции. Особо популярными стали массовые вирусные атаки, иногда принимающие характер эпидемий.

В подобной ситуации, защищаясь от массовых атак, сторона защиты руководствовалась парадигмой ***«цифровой крепости»***, правильно организованная оборона которой исключала проникновение противника сквозь периметр защиты. Успешность и состоятельность защиты основывалась на результатах ретроспективного анализа произошедших ранее инцидентов в предположении неизменности условий функционирования ИКС, применяемых в них информационных технологий и задействованных при этом программно-технических средств.

Но когда защита научилась эффективно отбиваться от массовых угроз, тенденция атак опять начала меняться: вновь стали реализовываться целевые атаки, но в более высоком профессиональном исполнении. И если против атак со стороны скрипт кидди парадигма «цифровой крепости» оставалась эффективной, для защиты от атак профессионала она оказалась несостоятельной.

Это стало очевидным около десяти лет назад, на рубеже первого десятилетия XXI века, когда ряд успешных атакующих действий практически доказал невозможность в рамках требований большинства традиционных руководств по менеджменту безопасности информации, основывающихся на анализе и исследовании имевших место ранее инцидентов и учете свойств ретроспективно выявленных угроз, обеспечить необходимый уровень безопасности информации.

Данный вывод привел к постулированию новой парадигмы: ***информационная система может быть и будет взломана*** [17]. Специалистами по безопасности эта парадигма воспринималась по-разному, главным образом из-за различий в толковании (понимании) ее содержания. Некоторые видели необходимость смещения акцентов защиты в сторону обеспечения непрерывности бизнес-процессов, оставления эффективных аварийно-восстановительных планов, уменьшения нанесенного ущерба за счет реализации комплекса действий, охватывающего весьма обширный перечень мероприятий, начиная с чисто технических вопросов резервного копирования, зеркалирования данных, восстановления информации, др. и до экономико-организационных мер, включающих передачу рисков, страхование и т.п.

Однако в большинстве случаев фактически суть новой парадигмы состояла в расширение сферы защитных действий, пресечении атак и устранении угроз как на границе периметра, так и после его преодоления: методология защиты изменялась, адаптируясь к текущему соотношению потенциалов и реальных возможностей сторон конфликта. Характерной особенностью парадигмы защиты стала реализация адаптивного управления безопасностью информации путем мониторинга возможных атак в режиме реального времени либо с незначительной задержкой, обусловленной потребностью в получении дополнительных сведений для принятия объективно обоснованного решения по данным мониторинга.

В частности, острая необходимость в обнаружении и анализе новых впервые появляющихся угроз (угрозы «нулевого» дня), реализовалась путем поиска и выделения поведенческих аномалий сред функционирования ИКС, использования песочниц, ловушек, других возможных средств и способов выявления атак.

Таким образом, для данной парадигмы очевиден переход от использования методологии, базирующейся на принципах контроля определенной совокупности статичных показателей, сохраняющих относительную устойчивость при реализации массовых (тиражируемых, повторяемых) атак, к динамическому (поведенческому) анализу угрозы, развивающейся в реальном времени.

Но упомянутые выше методы, более-менее оправдывающие себя при защите от целевых атак, быстро стали достаточно понятными для авторов современных атакующих технологий, что в итоге резко ухудшило ситуацию с защищенностью от сложных атак, реализуемых сегодня в киберпространстве, в частности, от направленных целевых атак класса APT.

Перспективной для этого случае представляется парадигма разработки систем защиты, базирующаяся на настойчиво декларируемых подходах и принципах ***проактивной защиты*** [14], [19]. К сожалению, единое общепринятое толкование этого термина пока отсутствует. В последнее время чаще всего под проактивной защитой понимаются действия упреждающего характера, предпринимаемые защищающцкйся стороной с целью обнаружения и предотвращения атак до того, как они приведут к каким-либо негативным последствиям. При этом, как уже отмечалось выше, для построения действительно стойкой системы безопасности недостаточно обеспечить безопасность периметра сети, необходимо также обеспечить контроль критически важных данных, производя мониторинг любых активностей в информационной системе и отслеживая все системные сообщения на предмет появления подозрительных изменений.

По оценкам специалистов [13], [17] многие сложные кибератаки оказываются невыявленными, а те, которые удалось обнаружить, не предаются огласке из-за репутационных рисков, в связи с чем предложить какую-либо типовую методику идентификации этих атак не представляется возможным даже для организаций, занимающихся расследованием инцидентов и анализом действий хакерских групп. Применяемые для обнаружения атак подходы часто базируются на использовании динамического анализа совокупности аномалий в состояниях различных элементов ИКС. Если эти аномалии удается увязать между собой в единую причинно-следственную цепоч-

ку, предложив правдоподобный сценарий развития сложной атаки, появляется реальная возможность прогноза ее негативных последствий с последующим применением классической методологии риск-ориентированного подхода для принятия решения о проведении адекватных защитных мероприятий.

Большинство результатов, получаемых в рамках подобной процедуры выявления и пресечения APT-угроз, носят преимущественно аналитический характер и формируются в SOC (Security Operations Center – оперативный центр безопасности) командой, состоящей в основном из аналитиков по безопасности, в задачи которых входит обнаружение и анализ инцидентов кибербезопасности, оперативное реагирование и предотвращение их возникновения, составление отчетности. Следует отметить существование других трактований понятия «проактивная защита», например [19]:

- атакующие действия, предпринимаемые против врага, готовящего нападение;

- упреждающая атака на основе доказательств того, что атака противника неизбежна;

- действия, предпринимаемые непосредственно против противника на превентивной стадии его атаки.

Очевидно, что при принятии любой из приведенных выше формулировок понятия «проактивная защита», непосредственному запуску процедуры (механизма) ее реализации должен предшествовать большой объм аналитической работы, выполняемой в SOC. Таким образом, вновь, как и тридцать три года назад (при организации и формировании CERT), основной акцент в обеспечении безопасности смещен в сторону экспертов-аналитиков, деятельность которых в идеале должна гарантировать адаптацию механизмов СЗИ к отражению любых сколь угодно сложных, постоянно изменяющихся угроз. Отличие в том, что SOC работает с внутренними инцидентами или инцидентами, направленными на внутренние информационные активы организации, а CERT обслуживает более высокий уровень анализа угроз, его сфера деятельности – ведомство, отрасль и выше.

Появлние SOC свидетельствует о том, что атаки профессионалов, в частности, сложные атаки класса APT, становятся достаточно распространенными. Это подтверждается и публикуемой статистикой. Если согласно классификации А.В.Лукацкого [7] в 2003 г. все атаки распределялись на «известные» и «неизвестные» в соотношении 95% / 5%, то в 2015 г. к «известным» и «неизвестным» добавились «сложные» атаки [12]: 70% / 29% / 1%, а в 2017 г. классификация приобрела вид [9]]: «обычные угрозы» - 90%, «сложные атаки» - 9%, «уникальные атаки» - 1%. Как видим, разделение атак на «известные» и «неизвестные» потеряло актуальность, а число «сложных атак» за два года увеличилось в 9 раз.

На первый взгляд приведенные данные говорят просто о росте количества и квалификации атакующих. Однако реальная ситуация качественно иная. В сфере кибератак образовался рынок услуг и аутсорсинга. Сегодня нет необходимости разрабатывать вредоносное ПО самостоятельно, тратить на разработку свое время и деньги - это уже обычный сервис, обеспечивающий атакующего достаточно развитым инструментарием (к примеру, покупка на Даркнет-рынке готовой к распространению версии шифровальщика, которую достаточно настроить и выпустить в сеть, или нового варианта трояна с уже продуманной стратегией распространения).

Становится актуальным применение аутсорсинговой модели в организации кибератак, когда хакеры производят кибератаки в качестве коммерческой услуги: в Даркнете появляются предложения об организации «коммерческих» DDoS-атак (можно заказать «положить сайт» за небольшую сумму, стоимость услуги зависит от мощности и продолжительности атаки), аренде ботсетей, продаже или аренде программных кодов вредоносного ПО, включая программы-шифровальщики (в 2015 г. появилась схема RaaS (Ransomware-as-a-service), посредством которой любой совершенно обычный пользователь может заказать услугу вредоносного заражения очень продвинутого уровня). Анализ многочисленных отчетов, обзоров, аналитических статей последних лет свидетельствует, что упомянутые

выше изменения в сфере кибератак стимулировали процесс интенсивного размывания компетентностных границ трех первых уровней ролевой классификации. В частности, для наиболее энергичных и подготовленных начинающих хакеров в сложившейся качественно новой ситуации стал возможным резкий рост уровня практических умений, эволюционирующих до сложных техник, что позволило им быстро, фактически минуя стадию «скрипт кидди», заявить о себе как о профессионалах. Последнее в свою очередь способствовало появлению и быстрому наращиванию мощного переходного резерва, представители которого «диффундируют» выше, в слой прфессионалов-исполнителей.

В целом злоумышленники становятся все более организованными и рациональными в отношении затрат на подготовку и проведение атак, минимизируя свои расходы, что способствует росту прибыльности атак и, как следствие, неминуемому увеличению их общего количества и разнообразия. Поэтому, при всей пафосности парадигмы проактивной защиты, идея предотвращения всех инцидентов до их возникновения неоправданно дорога и, следовательно, несостоятельна с точки зрения привлекаемых для ее реализации ресурсов. Существует множество инцидентов, которые дешевле устранить по факту их совершения, чем предотвращать в рамках проактивной парадигмы. Например, сейчас возросшая активность шифровальщиков ставит бизнес перед выбором: либо инвестировать значительные средства в безопасность, попытавшись в принципе исключить возможность атаки шифровальщика, либо ограничиться лишь реактивными защитными мерами, характерными для парадигмы неминуемого взлома защитного периметра.

Таким образом, реализация парадигмы проактивной защиты при своем практическом воплощении неизбежно сталкивается с необходимостью разумной балансировки проактивных и реактивных механизмов обеспечения безопасности информации. Базовыми сведениями, позволяющими провести эту балансировку, оставаясь в рамках экономически приемлемых инвестционных решений, являются рассчитанные для рефлексивных рисков (6) и (15) оценки максимального объема инвестиций $c_{eff\,\max}$ и разумного объема $\tilde{c}^{*}_{eff}$.

ВЫВОДЫ

Развитие ситуации в сфере защиты информации в ряде случаев целесообразно представить в форме модели двустороннего конфликта «атака/защита», где сторона защиты – владелец информации, цель которого - обеспечение безопасности принадлежащей ему информации от посягательств второго участника конфликта – стороны атаки, которая в реальности может представлять собой некоторое множество атакующих, действующих независимо либо в кооперации друг с другом. Конфликт носит процессный характер, активность проявляет сторона атаки, обновляя и совершенствуя применяемые ею методы и инструментарий, тем самым способствуя обеспечению эффективности и прибыльности своих действий. В итоге защищающаяся сторона вынуждена также постоянно модифицировать свою систему защиты, хотя выполнение защитных функций не является ее прямой задачей и носит обеспечивающий характер для успешной реализация основной деятельности организации-владельца информации. Поэтому для стороны защиты весьма важна задача минимизации инвестиций в СЗИ при сохранении приемлемых показателей устойчивости и безопастности своей основной деятельности.

Если при построении первых СЗИ нормой было перекрытие всех направлений реализации атак, то с ростом их количества стали блокироваться лишь актуальные (значимые) с точки зрения защищающейся стороны атаки, выделяемые (приоритизируемые) применением риск-ориентированного подхода, что в какой-то мере позволяло согласовать требования к безопасности с необходимостью выделения минимально необходимых объемов инвестиций в СЗИ.

Однако усложнение способов осуществления угроз привело к необходимости учета и анализа актуальности всех возможных атак, обусловив стремительное увеличение их общего числа, что в итоге сделало полноценное и несубъективное

применение риск-ориентированного подхода практически невозможным. Возникшую проблему разрешила смена защитной парадигмы. Новая парадигма упростила адаптацию методов и механизмов защиты к целевым рационально планируемым атакам, став одновременно для стороны атаки новым побудительным имульсом к разработке еще более сложных уникальных адресных атак класса APT. В свою очередь это опять подтолкнуло к внесению новых изменений в методологию защиты, формированию очередного обновления ее парадигмы и так далее, т.е. в итоге: идет процесс взаиморазвития обеих конфликтующих сторон, реализуемый за счет адаптации одной стороны к результатам практических действий другой (коадаптация). Следует отметить, что измение парадигмы не означает отрицания методов, технологий и механизмов, применявшихся сторонами на предшествовавших стадиях ее развития. Но здесь возникает проблема балансировки всех этих методов, технологий и механизмов без превышения экономически приемлемого объема суммарных инвестций в СЗИ. Для ее разрешения предлагается адаптивный подход к построению СЗИ, базирующийся на:

- введении набора вербальных ролевых моделей типовых сценариев поведения атакующей стороны;

- формировании рефлексивных моделей рисков, представляющих собой математические модели рисков для введенных выше типовых сценариев поведения атакующей стороны, в которых учитываются характеристики обеих сторон информационного конфликта;

- использовании рефлексивных моделей рисков для расчета базовых показателей СЗИ, в частности, оценочного значения предельного объема инвестирования;

- согласовании финансово-экономических возможностей организации с ее требованиями и возможностями в сфере защиты информации, обеспечении эффективного и рационального инвестирования в СЗИ и формирование ее структуры.

ЛІТЕРАТУРА

[1] Архипов А.Е. Применение среднего риска для оценивания эффективности защиты информационных систем. // *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ-2007р, випуск 3(14).- С. 60-67.

[2] Архипов О.Є. *Вступ до теорії ризиків: інформаційні ризики: монограф.* / О.Є.Архипов. - К.: Нац. Академія СБУ, - 2015 - 248 с.

[3] Архипов А.Е. Применение рефлексивных моделей рисков для защиты информации в киберпространстве // А.Е.Архипов. *Захист інформації*. – 2017. - Том 19, №3. – С. 204-213.

[4] Архипов А.Е. Риск-ориентированный поход к оцениванию «разумного» объема инвестиций в системы защиты информации // *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ – 2018 р., випуск 1(35). - 158 с., С. 18-29.

[5] Архипов А.Е., Архипова С.А. Адаптивные аспекты построения систем защиты информации // *Безпека ресурсів інформаційних систем*: збірник тез І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Чернігів: НУЧП, 2020. – С. 37-43.

[6] *Информационная безопасность банковских безналичных платежей*. Часть 4 - Обзор стандартов моделирования угроз. [Электронный ресурс] – Режим доступа: https://habr.com/ru/post/3513 26/.

[7] Лукацкий А.В. *Обнаружение атак*. – СПб.: БХВ – Петербург, 2003. – 608 с.

[8] Макнамара Д. *Секреты компьютерного шпионажа: Тактика и контрмеры*. М.: БИНОМ. Лаборатория знаний. - 2004. – 536 с.

[9] *Передовая защита от сложных угроз и снижение риска целевых атак. 2017*. [Электронный ресурс] – Режим доступа: https://media.kaspersky.com/ pdf/ APT_Report_ONLINE_AW_rus.pdf.security/Kaspersky_Anti_Targeted_Attack_Platform_Whitepaper_RU.pdf.

[10] *Руководство по управлению рисками безопасности. Группа разработки решений Майкрософт по безопасности и соответствию регулятивным нормам*, Центр Microsoft security center of excellence.[Электронный ресурс] – Режим доступа: http://infoeto.ru/ download/rukovodstvo-po-upravleniyu-riskami-bezopasnosti.doc.

[11] Столлингс В. *Основы защиты сетей. Приложения и стандарты*. - М.: Издательский дом «Вильямс», 2002. – 432 с.

[12] *Угрозы будущего: будьте к ним готовы. Специальный отчет о стратегиях борьбы со сложными угрозами. 2015* [Электронный ресурс] – Режим доступа: https://media.kaspersky.com/pdf/APT_Report_ONLINE_AW_rus.pdf.

[13] Целенаправленные атаки - маркетинговый термин или изощренный тип атак? // *!Безопасность Деловой Информации*, №6, 2014. – 58 с. [Электронный ресурс] – Режим доступа: https://www.twirpx.com/file/1636144/.

[14] Colbaugh R. Glass K Proactive Defense for Evolving Cyber Threats. *Sandia National Laboratories Albuquerque*, New Mexico 87185 and Livermore, California 94550 Unlimited Release Printed November 2012 [Electronic resource] - Access mode: https://www.google.com/search?client=avast&q=Proactive+Defense+for+Evolving+Cyber+Threats+Colbaugh+R.+ristin+Glass+K.

[15] Dorothy E. Denning. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy // *Global Problem Solving Information Technology and Tools*, December 10, 1999, https://nautilus.org/global-problem-solving/ activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/.

[16] Gordon, L.A., and Loeb, M.P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and Systems Security*, 5(4), 438-457.

[17] Hayden E. The New Paradigm for Utility Information Security: Assume Your Security System Has Already Been Breached. *Asian Power*. [Electronic resource] - Access mode: http://ca.reuters.com/article/technologyNews/idCATRE6BF6BZ201012 16.

[18] Huang, Hu, Behara. Economics of Information Security Investment in the Case of Simultaneous Attacks: Proceedings of the Fifth *"Workshop on the Economics of Information Security"*. June 26-28, Cambridge, England. [Electronic resource] - Access mode: https://www.researchgate.net/publication/228612670_Economics_of_information_security_investment_in_the_case_of_simultaneous _attacks.

[19] Saini Hemraj, Saini Dinesh Proactive cyber defense and reconfigurable framework for cyber security. *International Review on Computers and Software*, March 2007, Vol.4. No.1 [Electronic resource] - Access mode: https://www.researchgate.net/publication/288516946_Proactive_cyber_defense_and_reconfigurable_framework_for_cyber_security.

АДАПТИВНИЙ ПІДХІД ДО ПОБУДОВИ І ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянуто застосування адаптивного підходу до побудови та забезпечення функціонування ефективної системи захисту інформації (СЗІ), що створюється організацією-власником інформаційного ресурсу в конфліктній ситуації «атака / захист», яка виникає при реалізації атакуючої стороною загроз щодо ресурсу, який підлягає захисту. Аналізується зміст основних концепцій адаптивного управління системою захисту інформації на різних стадіях розвитку інформаційних технологій, зокрема, забезпечення адекватних трансформацій парадигми захисту, обумовлених змінами в стратегії і тактиці дій атакуючої сторони. Досліджуються особливості та можливості практичного застосування нових концепцій захисту, наприклад таких, що передбачають неспроможність вимоги щодо вжиття заходів для запобігання можливого небезпечного інциденту в разі невиправданої дорожнечі їх здійснення порівняно з оцінкою ризику втрат, що виникають в результаті реалізації інциденту. Пропонується застосування підходу, суть якого полягає у використанні при створенні та управлінні СЗІ відомостей про особливості і характер поведінки обох сторін-учасників конфлікту. Узагальнення та «пакування» зазначених відомостей реалізується в формі математичних моделей - рефлексивних ризиків, структура і набір яких визначаються виділеними типовими сценаріями розвитку ситуації «атака / захист». Аналіз і дослідження моделей дає оціночну інформацію, яка дозволяє забезпечити ефективне і раціональне інвестування в СЗІ організації, збалансувавши фінансово-економічні можливості організації з її вимогами і можливостями в сфері захисту інформації.

Ключові слова: інформаційна система, система захисту, адаптація, пріоритизація, загрози, атаки, уразливості, ризики, ризик-орієнтований підхід, рефлексивна модель, пардигма захисту.

ADAPTIVE APPROACH TO CONSTRUCTION AND ENSURING THE FUNCTIONING OF INFORMATION SECURITY SYSTEMS

The application of an adaptive approach to the construction and operation of an effective information security system (ISS) created by an organization-owner of an information resource in an "attack / defense" conflict situation arising when the attacker implements threats against the protected resource is considered. The content of the basic concepts of adaptive management of the information security system at various stages of information technology development is analyzed, in particular, the provision of adequate transformations of the defense paradigm caused by changes in the strategy and tactics of the attacker's actions. The features and possibilities of practical application of new concepts of protection are investigated, for example, assuming the insolvency of the requirement to take measures to prevent a possible dangerous incident in the event of unjustified high cost of their implementation in comparison with the assessment of the risk of losses as a result of the implementation of the incident. The application of an approach is proposed, the essence of which is to use information about the characteristics and nature of the behavior of both parties to the conflict in the creation and management of information security systems. Generalization and "packing" of the specified information is realized in the form of mathematical models - reflexive risks, the structure and set of which are determined by the selected typical scenarios for the development of the "attack / defense" situation. Analysis and research of models provides evaluative information that allows to ensure effective and rational investment in the organization's information security system, balancing the financial and economic capabilities of the organization with its requirements and capabilities in the field of information protection.

Key words: information system, protection system, adaptation, prioritization, threats, attacks, vulnerabilities, risks, risk-based approach, reflexive model, protection paradigm.

Архипов Олександр Євгенійович, д.т.н., професор, професор кафедри інформаційної безпеки НТУУ «КПІ імені Ігоря Сікорського».
E-mail: sonet0515@gmail.com.
Orcid ID: 0000-0001-6832-2223.

Архипов Александр Евгеньевич, д.т.н., профессор, профессор кафедры информационной безопасности НТУУ «КПИ имени Игоря Сикорского».

Arkhypov Olexander Evgeniyovich, Dr.Sci.Tech., professor at the Department of Information Defense, NTUU «Igor Sikorsky Kyiv Polytechnic Institute».

DOI: 10.18372/2410-7840.23.15431
УДК 004.056

УДОСКОНАЛЕНИЙ МЕТОД АВТОМАТИЧНОГО АКТИВНОГО АНАЛІЗУ ЗАХИЩЕНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ

Роман Киричок, Ольга Зінченко, Ірина Срібна, Віталій Марченко, Олег Кітура

У статті запропоновано удосконалений метод автоматичного активного аналізу захищеності корпоративної мережі. В основу даного методу покладено синтез математичної моделі аналізу кількісних характеристик процесу валідації вразливостей, методики аналізу якості роботи механізму валідації виявлених вразливостей корпоративної мережі та методу побудови нечіткої бази знань для прийняття рішень при валідації вразливостей програмних та апаратних платформ. Зокрема математична модель аналізу ґрунтується на поліномах Бернштейна та дозволяє описати динаміку процесу валідації вразливостей. Методика аналізу якості роботи базується на інтегральних рівняннях, що враховують кількісні характеристики досліджуваного механізму валідації вразливостей в певний момент часу, що дозволяє будувати закони розподілу показників якості процесу валідації вразливостей та кількісно оцінювати якість роботи механізму валідації виявлених вразливостей. Метод побудови нечіткої бази знань базується на використанні нечіткої логіки, що в свою чергу, дає можливість забезпечити отримання достовірної інформації про якість механізму валідації вразливостей непрямим шляхом та дозволяє формувати вирішальні правила прийняття рішень щодо реалізації тієї чи іншої атакуючої дії під час проведення активного аналізу захищеності корпоративної мережі. Це дозволяє, на відміну від існуючих підходів щодо автоматизації активного аналізу захищеності, абстрагуватися від умов динамічної зміни середовища, тобто постійного розвитку інформаційних технологій, що призводить до зростання кількості вразливостей та відповідних векторів атак, а також зростання готових до використання експлойтів вразливостей та їх доступності, і враховувати лише параметри якості самого процесу валідації вразливостей.

Ключові слова: *активний аналіз захищеності, корпоративна мережа, цільова система, валідація вразливостей, експлойт.*

ВСТУП

На сьогодні, одним із актуальних напрямів забезпечення кібербезпеки інформаційних систем та мереж є впровадження превентивних механізмів, серед який, найперспективнішими залишаються методи активного аналізу захищеності, що дозволяють не лише виявляти вразливості, але й валідувати їх, тобто підтверджувати можливість реалізації конкретної вразливості. При цьому, основними недоліками активного аналізу захищеності залишається обробка великого об'єму інформації, яка здебільшого здійснюється вручну експертами або звичайними адміністраторами, а відповідно і якість аналізу залежить від їхньої кваліфікації. Ще одним із недоліків, що є особливо критичним при аналізі захищеності великих мереж, зокрема корпоративних, це масовість перевірок знайдених вразливостей, що відповідно також призводить до збільшення загального часу проведення такого аналізу. Таким чином, враховуючи вищезазначені недоліки, набирає вагомості питання автоматизації процесу активного аналізу захищеності корпоративних мереж, зокрема процедури валідації виявлених вразливостей.

Аналіз останніх публікацій та досліджень свідчить про те, що питанням автоматизації процесу активного аналізу захищеності корпоратив-