Концептуальный подход к реализации подсистемы проактивной защиты оперативного центра обеспечения кибербезопасности

М. М. Путято[1], А. С. Макарян[2]
Кубанский государственный технологический университет
[1] putyato.m@gmail.com, [2] msanya@yandex.ru

***Аннотация*. В статье рассматриваются вопросы анализа и моделирования подсистемы проактивной защиты оперативного центра обеспечения кибербезопасности. Постоянно изменяющиеся условия информационной среды и глобального информационного пространства диктуют возможность автоматизированного или автоматического «приспособления» систем безопасности к требованиям современных программных комплексов. Основными задачами по организации интеграции комплексной системы обеспечения безопасности в оперативный центр обеспечения кибербезопасности и определения регламента взаимодействия с функциональными блоками является анализ и внедрение различных формализованных процедур обеспечения комплексной безопасности. Подсистема проактивной защиты комплексного обеспечения безопасности рассматривается, как объект, реализующий возможность управления и оперативного построения модели защиты в зависимости от решаемой задачи для предупреждения, или ликвидации инцидента.**

Предложенный подход продиктован не только повышением функциональности современных технологий, но и требованиями к созданию интегрированных решений, масштабируемых в рамках архитектуры для защиты от различного типа угроз. Использование комплексной системы обеспечения безопасности в рамках предложенного подхода позволит оперативно предотвращать инциденты как внешнего, так и внутреннего характера, что позволит своевременно нейтрализовать последствия их влияния.

Подсистема проактивной защиты обеспечит своевременный мониторинг, контекст и возможности предотвращения в различных ситуациях. Разработка такой платформы интеграции позволит улучшить автоматизацию и повысить качество информации, предоставляемой продуктами для обеспечения информационной безопасности.

Ключевые слова: комплексная безопасность; оперативный центр обеспечения кибербезопасности; информационная безопасность; проактивная защита; системы упреждения атак; модель с полным перекрытием; математическая модель

I. Введение

В сфере информационной безопасности существует большое количество математических и концептуальных моделей. Каждая из них предоставляет взгляд на определённый аспект процесса защиты информации. Например, модель Cyber Kill Chain описывает процесс атаки злоумышленника на информационную систему, который состоит из следующих этапов [1]:

- Разведка.
- Вторжение.
- Эксплуатация.
- Повышение привилегий.
- Боковое движение.
- Обфускация / Анти-криминалистика.
- Отказ в обслуживании.

Cyber Kill Chain позволяет построить эшелонированную, относительно этапов кибератаки, систему защиты информации, а также разделить все средства и методы защиты информации на проактивные и реактивные.

Проактивная защита подразумевает функционирование системы в постоянном ожидании угроз и их предотвращение до того, как они вступят во взаимодействие с объектом информатизации и смогут оказать на него влияние [2]. В контексте модели Cyber Kill Chain проактивная защита подразумевает препятствие развитию угроз до этапа Exploitation, включительно.

В свою очередь, реактивная защита подразумевает противодействие угрозам в процессе их реализации, а также минимизацию ущерба от вторжения. Проактивные и реактивные методы защиты не взаимозаменяемы. Надёжная система обеспечения информационной безопасности требует их совместного использования для эффективного противодействия угрозам на всех этапах их жизненного цикла [3].

Тем не менее, актуальные тенденции развития информационных технологий свидетельствуют о том, что проактивные методы защиты получают недостаточно внимания со стороны компаний. Их более широкое внедрение способно не только повысить качество защиты информации, но и снизить издержки.

Во-первых, только методы, препятствующие реализации угроз способны затруднить проведение неизвестных атак (угроз нулевого дня), а также сложных и

проработанных угроз, нацеленных на конкретный объект информатизации (advanced persistent threat) [5].

Во-вторых, проактивная защита нацелена на нейтрализацию угрозы до её реализации, что, в случае успеха, позволяет полностью исключить возможность негативного воздействия на информационную систему.

В-третьих, широкое разнообразие информационных технологий и быстрое появление новых типов угроз приводят к сложности масштабирования реактивных методов и уменьшению их эффективности. Например, сигнатурное сканирование, используемое антивирусами, подразумевает необходимость распознания каждой новой угрозы экспертами, внесение её в реестр угроз, обновление реестра, используемого каждым экземпляром антивируса и, в конце концов, сравнение наблюдаемого артефакта угрозы со всеми сигнатурами из реестра [6].

Воспользовавшись моделью Cyberkill chain, можно выделить следующие эшелоны методов проактивной защиты, в зависимости от того, на каком этапе развития кибератаки происходит противодействие.

ТАБЛИЦА I ЭШЕЛОНЫ МЕТОДОВ ПРОАКТИВНОЙ ЗАЩИТЫ

Эшелон проактивной защиты	**Этап атаки в модели Cyberkill chain**
Маскировка свойств объекта защиты	Reconaissance
Предотвращение утечки информации из объекта защиты	
Аудит	
Контроль и управление доступом к периметру информационной системы	Intrusion
Предотвращение вторжений	
Закрытие уязвимостей	Exploitation
Ограничение программной среды	
Контроль (анализ) защищенности информации	

II. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПОДСИСТЕМЫ ПРЕДОТВРАЩЕНИЯ УГРОЗ ОЦОК

Далее раскроем наполнение функциональных элементов подсистемы предотвращения угроз ОЦОК.

Применение интеллектуальных технологий для *обеспечения безопасности*. Традиционный алгоритм работы таких средств защиты информации как антивирусы, межсетевые экраны прикладного уровня и анализаторы уязвимостей опирается на сигнатурный подход. Сигнатурный подход подразумевает выявление угрозы, внесение экспертами новой сигнатуры в реестр угроз, а затем – обновление локальных экземпляров реестров средств защиты. Основной недостаток данного подхода заключается в том, что нейтрализовать угрозу будет возможно только после её первого обнаружения и обработки. Однако применение технологий искусственного интеллекта для анализа угроз позволяет обнаруживать угрозы нулевого дня.

Контроль функционирования подсистемы предотвращения угроз ОЦОК в различных режимах. Работа ОЦОК предусматривает переходы в различные режимы для создания оптимальной структуры, предназначенной для обеспечения эффективного взаимодействия и координации работы всех компонентов системы. В таком случае подсистема предотвращения угроз ОЦОК обеспечивает структурную, параметрическую и ситуационную безопасность при функционировании интегрированного комплекса как в режиме реального времени, так и в режиме offline [7].

Формирование новых моделей безопасности на основе систем моделирования и экспертного мнения. Одно из необходимых условий эффективности адаптивной защиты ОЦОК состоит в своевременной актуализации применяемых технологий защиты в соответствии с текущим ландшафтом угроз безопасности [7]. Для этого применяются системы имитационного, агентного и дискретно-событийное моделирования, а также экспертные системы, использование которых обеспечивает возможность уменьшения временных затрат, необходимых для принятия решения.

Организационно-правовое сопровождение. Согласно исследованию, проведённого лабораторией Касперского [8], подавляющее большинство инцидентов безопасности происходит ввиду человеческого фактора и недостаточной осведомлённости сотрудников о базовых правилах информационной безопасности. В связи с этим, организационно-правовое сопровождение является необходимой составляющей подсистемы предотвращения угроз ОЦОК.

Хранилище данных. Безопасность БД и ХД. Облачные технологии. Распределенные технологии передачи и хранения данных. Подсистема визуализации. Защита закрытой части, ОЦОК заключается в укреплении периметра для того, чтобы затруднить возможность его преодоления внешними угрозами [9]. Защита от внутренних угроз основывается на применении систем идентификации с использованием комбинированных методов доступа: биометрические, аппаратно-программные, организационные, пароли и ключи доступа.

Для анализа системы предотвращения угроз ОЦОК, с целью обеспечения её эффективной работы, выбрана модель с полным перекрытием [10], которая является разновидностью модели анализа угроз систем. Условием безопасности моделируемой системы защиты является наличие как минимум одного средства (субъекта) для обеспечения безопасности на каждом возможном пути проникновения в систему. Модель позволяет анализировать и подбирать количественные характеристики защищаемых объектов, действий злоумышленника и потенциального ущерба.

Модель с полным перекрытием отражает связь между «областью угроз», «системой защиты» и «защищаемой областью». Данная модель может быть описана совокупностью следующих множеств:

$T = \{ti\}$ – множество угроз;

$O = \{oj\}$ – множество объектов защищенной системы;

M = {mk} – множество механизмов безопасности ОЦОК.

Стандартная модель с полным перекрытием приведена на рис. 1.

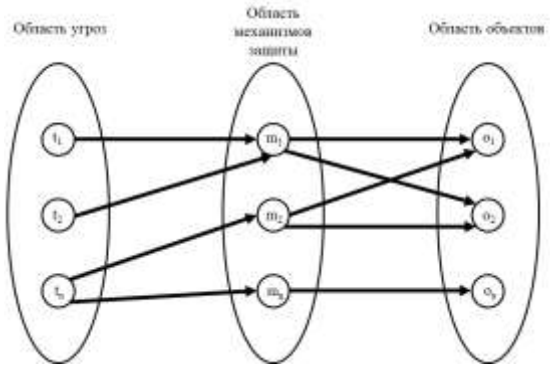

Рис. 1. Стандартная модель системы обеспечения безопасности с полным перекрытием в виде трехдольного графа

Система обеспечения безопасности описывается отношениями между элементами этих множеств. В качестве математического аппарата, позволяющего проиллюстрировать данные отношения, как правило, применяется графовая модель. При этом множество отношений угроза-объект образует двудольный граф. Задача реализации подсистемы предотвращения угроз состоит в том, чтобы перекрыть все существующие в графе рёбра. Это выполняется посредством добавления третьего набора – M.

В качестве перспективной новинки в области моделирования информационной безопасности выступает модель, уточняющая общую модель с полным перекрытием. Особенность дополненной модели заключается в введении набора уязвимостей – V и набора барьеров – B.

Уязвимость системы защиты – возможность осуществления угрозы ti в отношении объекта oj. Набор уязвимостей – V определяется подмножеством декартова произведения T*O: v_r=<t_i,o_j>.

Барьеры определяются декартовым произведением V*M: b = <t_i,o_j,m_k>. Под барьерами понимают пути осуществления угроз безопасности, перекрытые средствами защиты.

В системе с полным перекрытием для каждой уязвимости должен присутствовать барьер, препятствующий реализации соответствующих угроз.

Задача механизмов защиты – обеспечение сопротивляемости угрозам. В связи с этим, в качестве характеристик барьера может рассматриваться набор <P_i, D_i, R_i>, где P_i – вероятность появления i-ой угрозы, D_i – потенциальный ущерб при осуществлении i-ой угрозы, а R_i – степень сопротивляемости механизма защиты.

Прочность барьера характеризуется величиной остаточного риска X_i, связанного с возможностью осуществления угрозы t_i в отношении объекта o_j при использовании механизма защиты s_k.

$$X_i = P_k * D_k (1 - R_k). \quad (1)$$

Количественная характеристика защищенности рассчитывается по формуле:

$$Z = \frac{1}{\sum_{\forall b_k \in B} P_k * D_k (1 - R_k)}, \quad (2)$$

Однако, с практической точки зрения, получение точных значений приведённых характеристик барьеров представляет трудность в связи со сложностью формализации таких понятий как угроза, ущерб и сопротивляемость механизма защиты.

Безопасность информации, поддающейся оценке ущерба, целесообразно обеспечивать с использованием стоимостных методов оценки эффективности средств защиты. Отличительной особенностью этих методов является использование величины F_i, отражающей затраты на построение барьера b_i. Тогда определение оптимального набора СЗИ заключается в минимизации суммарных затрат A={a_i}, которые складываются из затрат на создание барьера F = {f_i} и потенциальных потерь, вызванных реализацией угроз N={n_i}.

Для увеличения точности моделирования предлагается применять адаптивную модифицированную модель с полным перекрытием. Данное нововведение обеспечит возможность использования множества математических моделей компонентов подсистемы предотвращения угроз ОЦОК. Это позволит более детально отобразить концептуальную структуру системы обеспечения безопасности и ещё на стадии проектирования системы оценить её эффективность.

Модифицированная модель системы обеспечения безопасности с полным перекрытием в виде пятидольного графа с включением множества адаптивных моделей приведена на рис. 2.

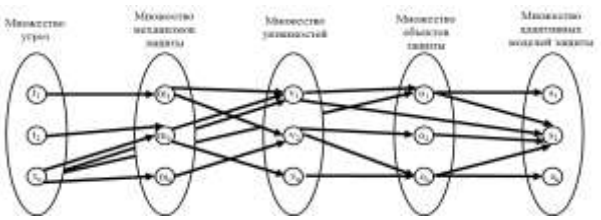

Рис. 2. Модифицированная модель системы обеспечения безопасности с полным перекрытием в виде пятидольного графа с включением множества адаптивных моделей

Приведённая модель предназначена для описания системы обеспечения безопасности в общем виде, однако, уточнив состав её компонентов, можно получить более конкретную модель, ориентированную на подсистему предотвращения угроз ОЦОК.

Модифицированная модель системы обеспечения безопасности с полным перекрытием в виде пятидольного графа с включением множества моделей предотвращения угроз на рис. 3.

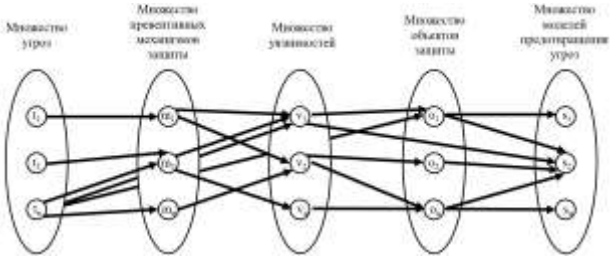

Рис. 3. Модифицированная модель подсистемы предотвращения угроз ОЦОК с полным перекрытием в виде пятидольного графа с включением множества моделей предотвращения угроз

Модель адаптивного управления подсистемой предотвращения угроз ОЦОК предлагается описывать формулой *Безопасность = Мониторинг + Аудит + Анализ риска + Политика безопасности + Средства защиты + Реализация контрмер*. Задача определения эффективности подсистемы предотвращения угроз складывается из определения перечня критериев эффективности и выбора методики их расчёта.

Для её решения предлагается использовать оптимизационный подход. При этом, под оптимизацией подразумевается максимизация значения некоторой функции при фиксированных ограничениях аргументов. Для обеспечения возможности применения данной методики к адаптивным подсистемам предотвращения угроз предлагается расширить её параметром k, означающей этап адаптивного процесса.

Введем следующие обозначения:

T = {t_j} – множество угроз безопасности, j = 1, … n;

$M^k = \{a_i^k\}$ – множество механизмов безопасности, используемых на k-м этапе адаптивного процесса, k = 0...R.

V = {v_i} – множество уязвимостей, i = 1…n.

$C^k = \{c_i^k\}$ – допустимые затраты на реализацию защиты объекта (объем затрат на сопровождение подсистемы предотвращения угроз с учетом реализации k-го этапа адаптивного процесса), где c_i – затраты на начальную разработку, обучение и запуск адаптивной системы;

$d^k(i,j)$ – эффективность нейтрализации i-м механизмом безопасности j-й угрозы на k-м этапе.

С целью построения математической модели вводится переменную p(i,j), которая равна 1 в случае, если j-я угроза устраняется при i-м механизмом, и нулю – в противном случае. Также вводится переменная q такая, что

$$q(i,j) = \begin{cases} 1 - \text{если}, i - \text{ый механизм без} - \text{ти} \\ \text{используется для устранения } j - \text{й угрозы} \\ 0 - \text{в противном случае} \end{cases} \quad (3)$$

В случае, если угрозы не связаны друг с другом, необходимо найти максимальный эффект от нейтрализации множества угроз T с помощью используемых в системе средств защиты S, с учётом заданных ограничений для затрат C.

$$\sum_{k=1}^{r} \sum_{j=1}^{m} \sum_{i=1}^{n} d^k(i,j) p(i,j) \to max \quad (4)$$

при ограничениях

$$\sum_{i=1}^{n} c(i) * sign \sum_{u_j \in U}^{n} p(i,j) \le C \quad (5)$$

$$p(i,j) \in (1,0)$$

Другой способ оценки эффективности подсистемы предотвращения угроз ОЦОК заключается в применении нечётких показателей. Пусть W – конечное множество показателей $W = \{w_i\}$, i=1..h, где h – количество показателей. Принадлежность к определенному уровню безопасности определяется на заданном промежутке $[0, T]$. Тогда множество значений модели S, оценивающей выполнение требований безопасности определяется как: $S = \sum_{i=1}^{n} \frac{\mu^A(x_i)}{x_i}$, где $\frac{\mu^A(x_i)}{x_i}$ – пара «функция принадлежности/элемент».

Различные подмножества нечёткого множества в этой модели представляют разные состояния безопасности. Вероятность реализации угрозы для оцениваемой системы, в таком случае, соответствует мощности выбранного нечёткого подмножества. При использовании данного подхода для оценки эффективности защищённости подсистемы предотвращения угроз ОЦОК требуется обладать данными об имеющихся требованиях защищённости и полноте выполнения этих требований. Предполагается, что данный подход позволяет обеспечить непрерывный мониторинг состояния подсистемы предотвращения угроз ОЦОК, прогнозирование возможности реализации угроз, возможность изменения требований к переменным безопасности, анализ условий, приводящих к появлению уязвимостей.

III. Заключение

В результате анализа основных функций и характеристик подсистемы предотвращения угроз ОЦОК были получены следующие выводы:

- проактивная защита, заключающаяся в предотвращении угроз до того, когда они смогут оказать влияние на систему, является перспективным направлением развития методов и средств информационной безопасности
- проактивный подход к защите приспособлен к созданию адаптивных интегрированных решений, масштабируемых в рамках архитектуры для защиты от различного типа угроз
- на основе модели Cyber Kill Chain выделены эшелоны проактивной защиты
- составлена концептуальная модель подсистемы предотвращения угроз ОЦОК, позволяющая оценить её количественные и качественные характеристики.
- составлена структурная модель подсистемы предотвращения угроз ОЦОК.

СПИСОК ЛИТЕРАТУРЫ

[1] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains // Lockheed Martin Corporation, Bethesda, 2010. p. 14.

[2] Richard Colbaugh, Kristin Glass, Proactive Defense for Evolving Cyber Threats (Sandia National Laboratories, Albuquerque, 2012) pp. 38-60.

[3] Craig, Amanda, Shackelford, Scott J., Hiller, Janine S., Proactive cybersecurity: a comparative industry and regulatory analysis // American Business Law Journal, 2015. p. 63.

[4] Kunwar Singh Vaisla, Reenu Saini, Analyzing of Zero Day Attack and its Identification Techniques // Proceedings of First International Conference on Advances in Computing & Communication Engineering (ICACCE-2014), 2014. p. 3.

[5] Ibrahim Ghafir, Vaclav Prenosil, Advanced Persistent Threat Attack Detection: An Overview // International Journal of Advancements in Computer Networks and Its Security, vol. 4, issue 4, 2014. pp. 50-54.

[6] Catalin Boja, Adrian Visoiu, Optimization of Antivirus Software // Informatica Economica Journal, issue 4(40), 2007. pp. 99-102.

[7] Путято М.М., Макарян А.С. Адаптивная система комплексного обеспечения безопасности как элемент инфраструктуры ситуационного центра // Прикаспийский журнал: управление и высокие технологии. 2020. №. 4 (52). С. 75-84.

[8] Kaspersky Lab. "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within". Available at: https://www.kaspersky.com/blog/the-human-factor-in-it-security/, last accessed 20.04.2021.

[9] Cristea Lavinia Mihaela, Current security threats in the national and international context // Journal of Accounting and Management Information Systems, vol. 19, issue 1, 2020. pp. 351-378.

[10] Максименко В.Н., Ясюк Е.В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. 2017. №. 2. С. 42-48.