РОССИЙСКАЯ АКАДЕМИЯ НАУК
Центр исследований проблем безопасности
АКАДЕМИЯ ВОЕННЫХ НАУК
Центр проблем стратегических ядерных сил

ИВ
ISSN 1996-4544

ИНФОРМАЦИОННЫЕ ВОЙНЫ

1–2019

ИНФОРМАЦИОННЫЕ ВОЙНЫ № 1(49) 2019

Научно-практический междисциплинарный журнал

Теория войн, информационное противоборство, информационный менеджмент, управление конфликтами и рисками, информационная безопасность, образование, математическая психология, вопросы истории.

Группа специальностей: политология (23.00.00).
Политические, социологические науки.

РОССИЙСКАЯ АКАДЕМИЯ НАУК
ЦЕНТР ИССЛЕДОВАНИЙ ПРОБЛЕМ БЕЗОПАСНОСТИ

АКАДЕМИЯ ВОЕННЫХ НАУК
ЦЕНТР ПРОБЛЕМ СТРАТЕГИЧЕСКИХ ЯДЕРНЫХ СИЛ

Издается с апреля 2007 г.
Свидетельство о регистрации
ПИ № ФС77-28172
от 28 апреля 2007г.

ISSN 1996-4544

Выходит 4 раза в год

СОДЕРЖАНИЕ

Для аспирантов и адъюнктов
публикация статей в журнале бесплатная.

Журнал включен
в «Перечень ведущих периодических изданий» ВАК.

IV. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056

© Василенко В.В., Сидак А.А.
© Vasilenko V., Sidak A.

УСТАНОВЛЕНИЕ ТРЕБОВАНИЙ И СИНЕРГИЯ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК

REQUIREMENTS DETERMINATION AND SYNERGY OF THE SYSTEM OF DETECTION, PREVENTION AND ELIMINATION OF CONSEQUENCES OF COMPUTER ATTACKS

Аннотация. *В статье изложены результаты анализа эволюции требований к защите от компьютерных атак. Показан синергетический эффект системы обнаружения, предупреждения и ликвидации последствий компьютерных атак для противостояния компьютерным атакам, развитие которых рассматривается как энтропийные тенденции. Предложено использование метода анализа иерархий для оценки значимости субъектов системы обнаружения, предупреждения и ликвидации последствий компьютерных атак для снижения энтропии компьютерных атак по отношению к критической информационной инфраструктуре Российской Федерации.*

Abstract. *The article presents the results of the analysis of computer attacks protection requirements evolution. The synergistic effect of the system of detection, prevention and elimination of consequences of computer attacks to counter computer attacks, the evolution of which is regarded as entropic tendencies, is shown. It is proposed to use the hierarchy analysis method for assessing the significance of participants in the system of detection, prevention and elimination of consequences of computer attacks to reduce the entropy of computer attacks in relation to the critical information infrastructure of the Russian Federation.*

Ключевые слова. *Компьютерная атака, энтропия, система, обнаружение, предупреждение и ликвидация последствий, синергия, мониторинг, компьютерный инцидент, метод анализа иерархии, критическая информационная инфраструктура, требование безопасности.*

Key words. *MComputer attack, entropy, system, detection, prevention and elimination of consequences, synergy, monitoring, computer incident, hierarchy analysis method, critical information infrastructure, security requirement.*

Современные объекты критической информационной инфраструктуры (КИИ) являются сложными по своей структуре и используемым информационным технологиям. Эти факторы, а также подключение объектов КИИ к сетям общего пользования (в том числе к Интернет), концентрация больших объемов чувствительной информации, распределенный характер ее обработки, в том числе с применением различных мобильных устройств, вовлеченность большого количества пользователей делают объекты КИИ подверженными рискам реализации угроз безопасности информации [1–3].

Наиболее опасными угрозами для критической информационной инфраструктуры являются компьютерные атаки (КА).

В Доктрине информационной безопасности Российской Федерации [4] отмечается постоянное повышение сложности, увеличение масштабов и рост скоординированности компьютерных атак (кибератак) на объекты критической информационной инфраструктуры Российской Федерации.

В качестве наиболее известных реализаций кибератак можно привести кибератаки с использованием вредоносного программного обеспечения «WannaCry», «Petya» и др. Хотя указанные кибератаки носили массовый характер, но в то же время они не были направлены на какие-то конкретные объекты информационной инфраструктуры.

Значительно большую опасность по возможным последствиям представляют целенаправленные (таргетированные) киберугрозы. В качестве исторического примера реализации таргетированной киберугрозы можно привести организованную кибератаку на ядерные объекты Ирана в 2009–2010 гг., с использованием компьютерного вируса Stuxnet.

По оценкам экспертов, которые озвучил председатель правительства Российской Федерации Д.А. Медведев в ходе московского международного форума «Открытые инновации» (октябрь 2018 г.), потери России от кибератак в 2017 г. составили около 600 млрд. рублей.

Таким образом, обеспечение своевременного обнаружения компьютерных атак, принятие мер по их предупреждению и ликвидации последствий является важнейшим фактором обеспечения безопасности объектов критической информационной инфраструктуры.

Василенко Владимир Васильевич *– доктор технических наук, профессор, заместитель председателя, ООО «Центр безопасности информации», v.vasilenko@cbi-info.ru;*
Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя, ООО «Центр безопасности информации», sidak@cbi-info.ru.*

Vasilenko Vladimir *– doctor of technical sciences, professor, deputy chairman, Information Security Center LLC, v.vasilenko@cbi-info.ru;*
Sidak Alexey *– candidate of technical sciences, senior researcher, deputy chairman, Information Security Center LLC, sidak@cbi-info.ru.*

Вопросам защиты от компьютерных атак посвящено множество работ [5, 6] и разработаны специализированные типы средств защиты.

Основная проблема противостояния компьютерным атакам – это их энтропия. Операторы информационных систем (ИС), автоматизированных систем управления (АСУ), информационно-телекоммуникационных систем (ИТКС) не обладают достаточными знаниями и компетенцией, чтобы самостоятельно распознать и нейтрализовать компьютерные атаки во всем их многообразии.

Энтропия компьютерных атак не является их собственным свойством. Энтропия – это то, как оператор описывает (воспринимает, понимает) компьютерные атаки.

Большинство операторов воспринимают компьютерные атаки по видам контролируемых последствий компьютерных инцидентов: несанкционированный доступ, утечка данных, модификация (подмена) данных, отказ в обслуживании, нарушение функционирования (работоспособности) технических средств и систем, неправомерное использование вычислительных или иных ресурсов [7].

К одним и тем же последствиям могут приводить различные сочетания факторов компьютерных атак на разных стадиях их развития (микросостояния). Общее количество этих состояний огромно. Значит энтропия компьютерных атак для оператора ИС, определяемая выражением (1), также имеет высокое значение.

$$H = \log \Omega, \quad (1)$$

где Ω – число микросостояний факторов компьютерных атак, приводящих к макросостоянию в виде конкретных последствий, известных оператору ИС.

Очевидно, чем меньше энтропия компьютерных атак, тем более эффективно можно организовать противодействие компьютерным атакам.

В общем снижение энтропии можно добиться за счет применения инструментальных средств, включающих постоянно обновляемые базы знаний о компьютерных атаках, а также – за счет создания в масштабной организационно-технической структуры (системы), обеспечивающей аккумуляцию, развитие знаний о компьютерных атаках и распространение этих знаний среди участников.

В начале развития этого направления защита от компьютерных атак предполагала выделение и развитие из множества средств защиты информации (ЗИ) таких специализированных типов средств, как средства обнаружения компьютерных атак (СОА) [5, 6].

Уполномоченными федеральными органами исполнительной власти были выпущены требования к мерам [8, 9] и средствам [10] обнаружения компьютерных атак.

Как показывает практический опыт, некоторые кибератаки также можно нейтрализовать или блокировать за счет структуризации объектов информационной инфраструктуры, то есть изменения их структурно-функциональных характеристик ИС с целью локализации защищаемой информации, реализации эшелонированной защиты и ограничения последствий возможных компьютерных инцидентов [11].

В дальнейшем глобализация проблемы защиты от компьютерных атак привела к необходимости разработки и утверждения всеобъемлющей концепции системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) [12, 13] как совокупности взаимодействующих центров мониторинга, предполагающих применение, помимо СОА, средств мониторинга [7], контроля защищенности и т.п.

Важное законодательное закрепление ГосСОПКА получила в Федеральном законе Российской Федерации от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [14] и дальнейшее развитие в нормативных правовых актах уполномоченного федерального органа исполнительной власти (ФОИВ).

В целом в ГосСОПКА можно выделить:

- организационную составляющую;
- документальную составляющую;
- инструментальную составляющую.

Организационная составляющая ГосСОПКА включает (см. рис.1) центры, организованные по ведомственному (корпоративному) и территориальному принципам [13]. Можно выделить следующие уровни центров и сегментов ГосСОПКА:

- уровень ФОИВ (Национальный координационный центр по компьютерным инцидентам – НКЦКИ, региональные и территориальные центры);
- уровень органов государственной власти (ведомственные сегменты и центры);
- уровень государственных корпораций, операторов связи и иных организаций (корпоративные сегменты и центры).

Документальная составляющая ГосСОПКА включает [13]:

- нормативно-правовое обеспечение;
- научно-техническое обеспечение;
- организационно-штатное обеспечение.

Инструментальная составляющая проиллюстрирована на рис. 2.

Инструментарий мониторинга и управления компьютерными инцидентами подробно рассмотрен в работе [7] и апробирован в комплексе средств Neurodat.

Простое суммирование возможностей и преимуществ отдельных участников (субъектов ГосСОПКА) сверхаддитивного эффекта для направления защиты от компьютерных атак не дает (см. таблицу).

Для преодоления ограничений, указанных в таблице, нужны особые системообразующие (синергетические) связи в рамках ГосСОПКА, которые при кооперативных (совместных) действиях участников ГосСОПКА увеличивали бы общий эффект до величины большей, чем сумма эффектов, получаемых от этих же участников, действующих независимо [15].

Взаимодействие в рамках ГосСОПКА, направленное на получение синергетического эффекта, предусматривает:

- вертикальное взаимодействие (НКЦКИ – Головной центр – Подчиненный центр);
- горизонтальное (Головной центр – Головной центр и др.);
- взаимодействие на уровне инструментальных

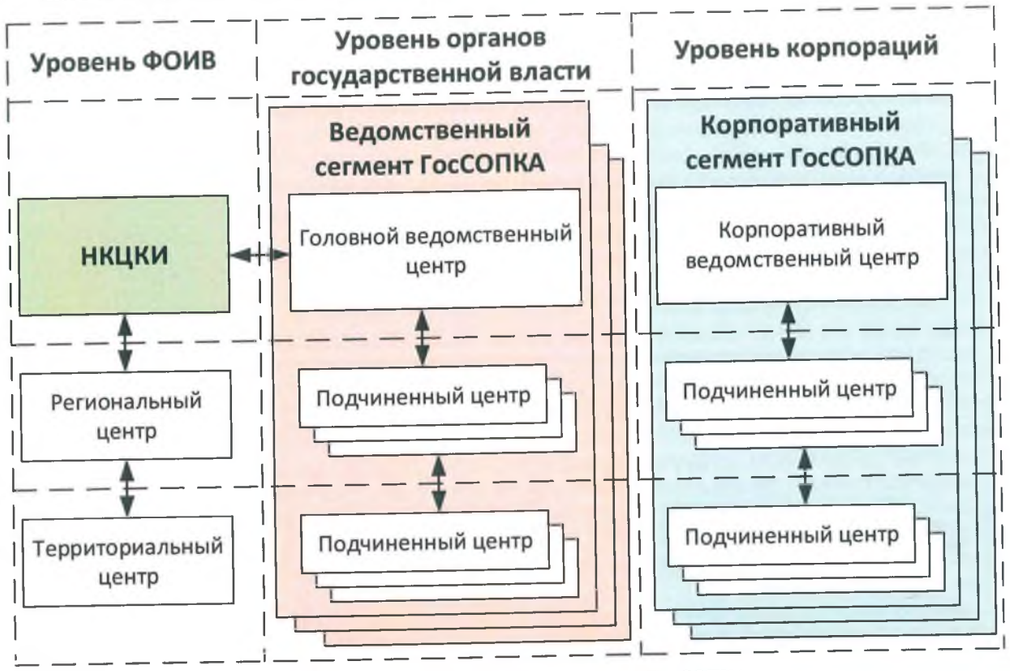

Рис. 1. Организационная составляющая Гос.СОПКА

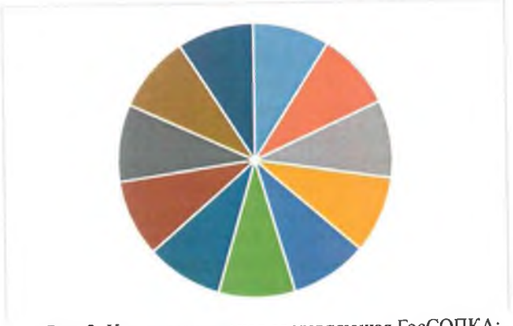

Рис. 2. Инструментальная составляющая ГосСОПКА:

средств;

- взаимодействие через базы знаний разработчиков (базы данных решающих правил, потоки данных об угрозах, содержащих индикаторы компрометации, справочники и т.п.).

Центры различных корпоративных (ведомственных) сегментов ГосСОПКА – это независимые друг от друга структурные единицы. Представляют информацию в НКЦКИ и друг другу, при этом обеспечивается синергетический (сверхаддитивный) эффект от использования ГосСОПКА.

Центры в рамках одного корпоративного (ведомственного) сегмента – также могут быть относительно независимыми. Синергетический эффект обеспечивается за счет целенаправленного регулирования со стороны головного центра.

Средства защиты, используемые в целях обнаружения, предупреждения и ликвидации последствий компьютерных атак, разных типов (СОА, мониторинг, средства анализа защищенности, средства мониторинга, «песочницы», средства антивирусной защиты, средства защиты от таргетированных атак средства и др.) в большинстве случаев являются независимыми. Синергетический эффект возникает, например, при объединении получаемой от них информации в SIEM-системах и системах управления компьютерными инцидентами типа Neurodat.

Таким образом, основное преимущество ГосСОПКА – это возможность снижения энтропии компьютерных атак за счет синергетического эффекта от кооперации участников ГосСОПКА (объединение знаний о компьютерных атаках, получение принципиально новых знаний и их широкого распространения среди участников).

Деятельность участников ГосСОПКА целесообразно оценивать. Безусловно, относительно собственного ведомственного (корпоративного) сегмента ГосСОПКА это оценка в терминах выполнения/невыполнения требований. В то же время с точки зрения вклада в синергетический эффект для всей ГосСОПКА (вклад в общее дело – снижение энтропии компьютерных атак),

Возможности и преимущества субъектов Гос.СОПКА

Участники	Преимущества	Потребности/ ограничения
Уполномоченный федеральный орган исполнительной власти	Имеет высшую компетенцию, знания и информацию о компьютерных атаках	Требуется: ▪ получение первичной информации от сегментов (центров); ▪ развитие системы распространения знаний и информации о КА
Операторы объектов КИИ	Имеют: ▪ первичную информацию мониторинга; ▪ информацию о последствиях компьютерных инцидентов (макросостояниях)	Не обладают: ▪ первичной информацией мониторинга конкретной ИИ; ▪ не имеют компетенций по корреляции событий безопасности для обнаружения КА
Разработчики средств ЗИ	Имеют знания о факторах КА, воплощенные в производимом продукте (средстве ЗИ) и базах знаний	Не обладают: ▪ первичной информацией мониторинга конкретной ИИ; ▪ не имеют компетенций по корреляции событий безопасности для обнаружения КА
Научное сообщество	Разрабатывает: ▪ типовые векторы КА; ▪ языки корреляции событий безопасности для обнаружения КА; ▪ способы применения искусственного интеллекта (нейросети и др.) для обнаружения КА	Отсутствуют: ▪ практически применимые цепочки событий безопасности (нормальные, аномальные); ▪ практическая реализация языков корреляции для масштабного применения в КИИ

участников надо сравнивать между собой. Наиболее подходящим экспертным методом для этого можно считать метод анализа иерархий [16]. При этом ключевым элементом применения данного метода является построение иерархии целей и задач предметной области для определения значимости (вклада) участников в снижение энтропии компьютерных атак.

В настоящее время взаимодействие НКЦКИ и субъектов ГосСОПКА может осуществляться посредством электронной почты или с использованием автоматизированных систем обмена информацией.

Очевидно, что дальнейшему снижению энтропии компьютерных атак будет способствовать повышение уровня взаимодействия именно автоматизированным способом. В этих целях в рамках линейки Neurodat, например, разработан специальный модуль взаимодействия, согласованы структура данных и формат обмена.

Литература

1. Сидак А.А. Определение актуальных угроз безопасности информации в автоматизированных системах// Двойные технологии, № 1, 2018, С. 73-75.
2. Сидак А.А., Ильин А.В., Кубарев А.В. Мобильные устройства в информационных системах и угрозы безопасности информации. Взаимосвязи// Вопросы кибербезопасности, №3, 2014. – С. 29-34.
3. Глухов А.П., Сидак А.А. Методологические аспекты управления рисками информационной безопасности ОАО «Российские железные дороги» // В сборнике: Интеллектуальные системы на транспорте: Сборник материалов V Международной научно-практической конференции «ИнтеллектТранс-2015»/ под редакцией д-ра техн. наук профессора А.А. Корниенко. – СПб.: ПГУПС, 2015. – С. 7-12.
4. Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 5.12.2016 № 646 // СПС КонсультантПлюс.
6. Климов С.М. Методы и модели противодействия компьютерным атакам. – Люберцы.: КАТАЛИТ, 2008. – 316 с.
6. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ, 2003. – 596 с.
7. Аксененко Ю.И., Василенко В.В., Сидак А.А. Методологический подход к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности// Стратегическая стабильность, № 1, 2018. – С. 64-67.
8. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», зарегистрирован в Минюсте России 31.05.2013 г. №28608 // СПС КонсультантПлюс.
9. Методический документ. Меры защиты информации в государственных информационных системах, утв. ФСТЭК России 11.02.2014 // СПС КонсультантПлюс.
10. Методический документ. Профили защиты систем обнаружения вторжений, утв. ФСТЭК России 3.02.2012: [Электронный ресурс] // ФСТЭК России, 2019. URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii-po-sertificatsii/120-normativnye-documenty/406-metodicheskie-documenty-utverzhdeny-fstek-rossii-3-fevralua-2012-g (Дата обращения: 31.01.2019).
11. Сидак А.А. Вопросы структуризации автоматизированных систем при организации защиты информации//