Синтез комплексной системы обнаружения компьютерных инцидентов безопасности в критических информационных инфраструктурах

А. А. Тихомирова, email: tihomirowaalina@yandex.ru [1]
А. В. Яковлев, email: yava73@bk.ru [2]
У. А. Савилова, email: yliana.savilova@gmail.com [3]

ФГБОУ ВО «Тамбовский государственный технический университет»

Аннотация. *Рассмотрена возможность синтеза комплексной системы обнаружения компьютерных инцидентов безопасности, возникающих на объектах критической информационной инфраструктуры.*

Ключевые слова: *компьютерный инцидент, критическая информационная инфраструктура, система обнаружения компьютерных инцидентов.*

Введение

Несмотря на высокий темп развития методов и средств защиты информации, количество инцидентов информационной безопасности с каждым годом только увеличивается. Особую опасность такие инциденты представляют для критической информационной инфраструктуры (КИИ).

КИИ – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия. В свою очередь, субъекты КИИ – это компании, работающие в стратегически важных для государства областях, а также организации, обеспечивающие взаимодействие систем или сетей КИИ.

В связи с государственной важностью обеспечения должного уровня защищенности КИИ, особую актуальность приобретает задача создания системы обнаружения компьютерных инцидентов безопасности в КИИ.

1. Компьютерные инциденты безопасности в КИИ

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения

безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

В соответствии с приказами ФСБ России от 24 июля 2018 г. №№366-368, субъекты КИИ и Национальный координационный центр по компьютерным инцидентам (НКЦКИ) осуществляют информационное взаимодействие, в ходе которого субъекты КИИ обязаны уведомлять НКЦКИ о компьютерных инцидентах, произошедших на объектах КИИ [1].

В целях унификации сведений, передаваемых в ходе информационного взаимодействия между НКЦКИ и субъектом КИИ, НКЦКИ и владельцами российских информационных ресурсов, НКЦКИ и иностранными (международными) организациями, выделяются базовые категории и типы компьютерных инцидентов, представленные в табл. 1.

Таблица 1

Базовые категории и типы компьютерных инцидентов безопасности

Категория компьютерного инцидента и его международное обозначение	**Тип компьютерного инцидента и его международное обозначение**
Заражение вредоносным программным обеспечением (malware)	Внедрение в контролируемый объект КИИ модулей вредоносного программного обеспечения (malware infection)
Распространение вредоносного программного обеспечения (malware distribution)	Использование контролируемого объекта КИИ для распространения вредоносного программного обеспечения (malware command and control)
Нарушение или замедление работы контролируемого информационного ресурса (availability)	Компьютерная атака типа «отказ в обслуживании», направленная на контролируемый объект КИИ (dos)
	Распределенная компьютерная атака типа «отказ в обслуживании», направленная на контролируемый объект КИИ (ddos)

Продолжение табл. 1

Категория компьютерного инцидента и его международное обозначение	**Тип компьютерного инцидента и его международное обозначение**
	Несанкционированный вывод объекта КИИ из строя (sabotage)
	Непреднамеренное отключение объекта КИИ (outage)
Несанкционированный доступ в систему (intrusion)	Успешная эксплуатация уязвимости на контролируемом объекте КИИ (application compromise)
	Компрометация учетной записи на контролируемом объекте КИИ (account compromise)
Сбор сведений с использованием информационно-коммуникативных технологий (information gathering)	Прослушивание (захват) сетевого трафика контролируемого объекта КИИ (traffic hijacking)
	Социальная инженерия, направленная на компрометацию объекта КИИ (social engineering)
Нарушение безопасности информации (information content security)	Несанкционированное разглашение информации, обрабатываемой на контролируемом объекте КИИ (unauthorised access)
	Несанкционированное изменение информации, обрабатываемой на контролируемом объекте КИИ (unauthorised modification)
Распространение информации с неприемлемым содержимым (abusive content)	Рассылка спам-сообщений с контролируемого объекта КИИ (spam)
	Публикация на контролируемом объекте КИИ запрещенной законодательством РФ информации (prohibited content)

Окончание табл. 1

Категория компьютерного инцидента и его международное обозначение	Тип компьютерного инцидента и его международное обозначение
Мошенничество с использованием информационно-коммуникативных технологий (fraud)	Злоупотребление при использовании объекта КИИ (unauthorized purposes)
	Публикация на контролируемом объекте КИИ мошеннической информации (phishing)

В табл. 1 представлены только базовые категории и типы компьютерных инцидентов безопасности, которые могут произойти на объектах КИИ. Однако в реальности КИИ подвержена огромному множеству различных по целям и характеру воздействия компьютерных инцидентов. Это означает, что создаваемая система обнаружения должна быть направлена на выявление как можно большего количества типов компьютерных инцидентов [2].

2. Существующие системы обнаружения компьютерных инцидентов безопасности в КИИ

В настоящее время решением задачи обеспечения информационной безопасности объектов КИИ занимается Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), структура которой представлена на рисунке

Рисунок. Структура ГосСОПКА

Структура ГосСОПКА включает в себя следующие элементы:

– главный центр ГосСОПКА (наивысшая структура в иерархии, разрабатывает нормативные документы и методики; за работу этого центра отвечает ФСБ России);

– головной центр ГосСОПКА (наивысшая структура в иерархии центров, объединённых по ведомственному или организационному признакам);

– центр ГосСОПКА (совокупность сил и средств субъекта ГосСОПКА, предназначенная для решения задач ГосСОПКА в своей зоне ответственности);

– подчинённый центр (центр, который структурно подчиняется головному центру);

– сегмент ГосСОПКА (совокупность головного центра и иерархически подчинённых центров);

– ведомственные центры (органы государственной власти).

– корпоративные центры (коммерческие и некоммерческие организации; могут оказывать услуги подключения к ГосСОПКА при наличии лицензии) [3-4].

ГосСОПКА предлагает различные варианты совместного противодействия компьютерным инцидентам безопасности. То есть, субъект КИИ может использовать готовые системы обнаружения компьютерных инцидентов безопасности, принадлежащие ведомственным или коммерческим центрам. Однако такой вариант не всегда в полной мере удовлетворяет требованиям информационной безопасности конкретного субъекта КИИ или же может не соответствовать его финансовым возможностям. Поэтому синтез собственной комплексной системы обнаружения компьютерных инцидентов безопасности может стать оптимальным вариантом обеспечения информационной безопасности КИИ.

3. Синтез комплексной системы обнаружения компьютерных инцидентов безопасности в КИИ

Осуществим синтез комплексной системы обнаружения компьютерных инцидентов безопасности в КИИ, которая будет направлена на выявление следующих категорий компьютерных инцидентов:

– заражение вредоносным программным обеспечением (malware);

– нарушение или замедление работы контролируемого информационного ресурса (availability);

– сбор сведений с использованием информационно-коммуникативных технологий (information gathering);

– несанкционированный доступ в систему (intrusion).

Составим множество альтернатив программных и программно-аппаратных средств, предназначенных для обнаружения вышеупомянутых компьютерных инцидентов, и занесем его в табл. 2.

Таблица 2

Множество альтернатив средств обнаружения инцидентов

Средства обнаружения инцидента malware	**Средства обнаружения инцидента availability**	**Средства обнаружения инцидента information gathering**	**Средства обнаружения инцидента intrusion**
Norton Antivirus Plus	Group-IB Fraud Hunting Platform	Kaspersky Anti Targeted Attack	Страж NT 4.0
McAfee Total Protection	Anti-DDoS Qrator	Kaspersky Industrial CyberSecurity	Secret Net 7
Kaspersky Total Security	CloudFlare DDoS Attack Protection	ViPNet IDS HS	ViPNet SafeBoot 1.4
Kaspersky Security Center 10	Kaspersky DDoS Protection	Kaspersky Private Security Network	Secret Disk 5
Dr.Web Enterprise Security Suite	ViPNet TIAS	Детектор атак «Континент»	Соболь 4.0
ESET NOD32 Secure Enterprise Pack	ViPNet IDS 2.0	Рубикон	vGate-S 4.1
Avira Total Security Suite	Cisco ASA FirePOWER 6.2	Аргус 1.5	Secret Net LSP

Произведем усечение множества альтернатив средств обнаружения компьютерных инцидентов по критерию «наличие сертификата ФСТЭК России».

Результат усечения множества альтернатив по заданному критерию представлен в табл. 3.

Таблица 3

Усечение множества альтернатив

Средства обнаружения инцидента malware	**Средства обнаружения инцидента availability**	**Средства обнаружения инцидента information gathering**	**Средства обнаружения инцидента intrusion**
Kaspersky Security Center 10	Kaspersky DDoS Protection	ViPNet IDS HS	Secret Net 7
Dr.Web Enterprise Security Suite	ViPNet TIAS	Детектор атак «Континент»	ViPNet SafeBoot 1.4
ESET NOD32 Secure Enterprise Pack	ViPNet IDS 2.0	Рубикон	Secret Disk 5
	Cisco ASA FirePOWER 6.2	Аргус 1.5	Соболь 4.0
			Secret Net LSP

Для синтеза комплексной системы обнаружения компьютерных инцидентов безопасности в КИИ воспользуемся методом парного сравнения

Метод парного сравнения – один из инструментов оценки и выбора решений, широко используется в экспертных оценках при необходимости расставлять приоритеты в процессе какой-либо деятельности или ранжирования различных объектов [5].

Парное сравнение альтернатив средств обнаружения заражения вредоносным программным обеспечением представлено в табл. 4. Один балл получает наименее дорогостоящая альтернатива (учитывается стоимость программного или программно-аппаратного средства на один персональный компьютер) с учетом качественных характеристик средств обнаружения.

Таблица 4

Сравнение альтернатив средств обнаружения заражения вредоносным программным обеспечением

Альтернатива	Kaspersky Security Center 10	Dr.Web Enterprise Security Suite	ESET NOD32 Secure Enterprise Pack	Сумма баллов

Окончание табл. 4

Kaspersky Security Center 10	–	1	1	2
Dr.Web Enterprise Security Suite	0	–	0	0
ESET NOD32 Secure Enterprise Pack	0	1	–	1

Таким образом, лучшей альтернативой средства обнаружения заражения вредоносного программного обеспечения для синтезируемой системы является Kaspersky Security Center 10.

Парное сравнение альтернатив средств обнаружения компьютерных инцидентов, направленных на нарушение или замедление работы контролируемого информационного ресурса, представлено в табл. 5.

Таблица 5

Сравнение альтернатив средств обнаружения инцидентов нарушения или замедления работы контролируемого информационного ресурса

Альтернатива	Kaspersky DDoS Protection	ViPNet TIAS	ViPNet IDS 2.0	Cisco ASA FirePOWER 6.2	Сумма баллов
Kaspersky DDoS Protection	–	1	0	0	1
ViPNet TIAS	0	–	0	0	0
ViPNet IDS 2.0	1	1	–	1	3
Cisco ASA FirePOWER 6.2	1	1	0	–	2

Таким образом, лучшей альтернативой средства обнаружения компьютерных инцидентов нарушения или замедления работы контролируемого информационного ресурса для синтезируемой системы – ViPNet IDS 2.0.

Парное сравнение альтернатив средств обнаружения несанкционированного сбора сведений с использованием информационно-коммуникативных технологий представлено в табл. 6.

Таблица 6

Сравнение альтернатив средств обнаружения несанкционированного сбора сведений

Альтернатива	ViPNet IDS HS	Детектор атак «Континент»	Рубикон	Аргус 1.5	Сумма баллов
ViPNet IDS HS	–	1	1	1	3
Детектор атак «Континент»	0	–	0	1	1
Рубикон	0	1	–	0	1
Аргус 1.5	0	0	1	–	1

Таким образом, лучшей альтернативой средства обнаружения несанкционированного сбора сведений с использованием информационно-коммуникативных технологий для синтезируемой системы является ViPNet IDS HS.

Парное сравнение альтернатив средств обнаружения несанкционированного доступа в систему представлено в табл. 7.

Таблица 7

Сравнение альтернатив средств обнаружения несанкционированного доступа в систему

Альтернатива	Secret Net 7	ViPNet SafeBoot 1.4	Secret Disk 5	Соболь 4.0	Secret Net LSP	Сумма баллов
Secret Net 7	–	1	1	1	1	4
ViPNet SafeBoot 1.4	0	–	0	1	1	2
Secret Disk 5	0	1	–	1	1	3
Соболь 4.0	0	0	0	–	1	1
Secret Net LSP	0	0	0	0	–	0

Таким образом, лучшей альтернативой средства обнаружения несанкционированного доступа для синтезируемой системы будет Secret Net 7.

Таким образом, синтезируемая комплексная система обнаружения компьютерных инцидентов состоит из следующих средств обнаружения компьютерных инцидентов безопасности:

- Kaspersky Security Center 10;
- ViPNet IDS 2.0;
- ViPNet IDS HS;
- Secret Net 7.

Заключение

Полученная комплексная система обнаружения компьютерных инцидентов безопасности в КИИ направлена на выявление как минимум четырех наиболее распространённых категорий компьютерных инцидентов. Основными преимуществами синтезированной системы является невысокая стоимость и возможность ее адаптации под конкретные требования субъекта КИИ.

Список литературы

1. Нормативные документы в области ГосСОПКА и безопасности КИИ [Электронный ресурс]. – Режим доступа : https://www.ptsecurity.com/ru-ru/research/knowledge-base/terminology-gossopka-kii-full-version/

2. Состав технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, и форматы представления информации о компьютерных инцидентах [Электронный ресурс]. – Режим доступа : https://safe-surf.ru/specialists/article/5252/638030/

3. ГосСОПКА [Электронный ресурс]. – Режим доступа: https://www.infosec.ru/glavnye-temy/gossopka/

4. Комплексное решение для создания центра ГосСОПКА и взаимодействия с НКЦКИ [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/solutions/center-gossopka/

5. Метод парных сравнений [Электронный ресурс]. – Режим доступа: https://hr-portal.ru/article/metod-parnyh-sravneniy