БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 4 (115). – 84–102

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056 DOI: 10.17212/2782-2230-2024-4-84-102

ВОПРОСЫ СБОРА ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ С УЗЛОВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В РАМКАХ ОСУЩЕСТВЛЕНИЯ МОНИТОРИНГА БЕЗОПАСНОСТИ*

М.А. МАРЧЕНКО[1], Р.А. ПЕРМЯКОВ[2], И.А. ОГНЕВ[3], И.В. НИКРОШКИН[4]

[1] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики СО РАН, доктор физико-математических наук, профессор РАН, директор лаборатории искусственного интеллекта и информационных технологий. E-mail: marchenko@sscc.ru*

[2] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики СО РАН, ведущий инженер лаборатории искусственного интеллекта и информационных технологий. E-mail: pra@sscc.ru*

[3] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики СО РАН, инженер лаборатории искусственного интеллекта и информационных технологий. E-mail: ognev.igor.alex@gmail.com*

[4] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Институт вычислительной математики и математической геофизики СО РАН, инженер лаборатории искусственного интеллекта и информационных технологий. E-mail: ivan.nikroshkin@bk.ru*

В настоящее время растет роль процесса мониторинга событий безопасности информационных систем, в том числе и распределенных информационных систем. Средства защиты информации, включая и узловые средства защиты информации, являются основными источниками событий информационной безопасности для систем мониторинга безопасности. Не все представленные в настоящее время узловые средства защиты информации одинаково полезны и информативны как источники событий информационной безопасности для систем мониторинга. В данном исследовании поднимаются вопросы оценки эффективности узловых средств защиты информации как источников событий информационной безопасности. Предлагаемая оценка эффективности основана на анализе способности узловых средств защиты информации детектировать различные модели распространения последствий компьютерных инцидентов, а также на способности детектирования определенных техник и тактик злоумышленников, которые они ис-

* Статья получена 02 декабря 2024 г.

Работа выполнена в рамках государственного задания ИВМиМГ СО РАН № FWNM-2022-0005.

пользуют для реализации компьютерных атак, влекущих за собой компьютерные инциденты. В рамках настоящего исследования были рассмотрены следующие узловые средства защиты информации: системы защиты информации от несанкционированного доступа, средства антивирусной защиты информации, узловые системы обнаружения и предотвращения вторжений, средства защиты конечных устройств, системы автоматического выявления и устранения вредоносной активности на конечных устройствах, системы контроля целостности, системы предотвращения утечек информации. Сформированная оценка эффективности узловых средств защиты информации как источников событий безопасности позволяет реализовать более эффективные системы защиты информации и процесс мониторинга событий безопасности за счет устранения избыточных событий информационной безопасности, которые могут привести к ложным срабатываниям и перегрузке систем мониторинга. Кроме того, на базе методики и анализа существующих типов узловых средств защиты информации были сформированы рекомендации, направленные на повышение уровня защиты информационной инфраструктуры организаций, что способствует созданию более адаптивной и динамичной системы противодействия угрозам.

Ключевые слова: средства защиты информации, узловые средства защиты информации, эффективность, мониторинг, мониторинг безопасности, информационная безопасность, кибербезопасность, модели распространения последствий компьютерных инцидентов

ВВЕДЕНИЕ

Несмотря на значимость узловых средств защиты информации для процесса мониторинга событий информационной безопасности, не все они обладают равной степенью полезности и информативности [1, 2]. Некоторые из них могут быть более эффективными в определенных условиях или против конкретных типов угроз, в то время как другие могут предоставлять избыточные или нерелевантные данные, затрудняя их интерпретацию. Кроме того, различные узловые средства могут различаться по уровню автоматизации и интеграции с другими системами, что влияет на их способность быстро и адекватно реагировать на выявленные угрозы. При выборе и использовании таких средств необходимо учитывать их соответствие специфическим требованиям и характеристикам защищаемой системы [3, 4], а также их взаимодействие с другими мерами защиты [5], что позволит повысить общий уровень безопасности информационной системы.

Цель исследования – формирование оценки эффективности узловых средств защиты информации как источников события для систем мониторинга информационной безопасности. В рамках достижения цели были рассмотрены следующие вопросы: описание типов узловых средств защиты информации и видов событий, их значения для средств мониторинга событий информационной безопасности, формирование критериев эффективности

узловых средств защиты информации и генерируемых ими типов событий, проведение аналитического сравнения узловых средств защиты информации и генерируемых ими типов событий по разработанным критериям.

1. КЛАССИФИКАЦИЯ УЗЛОВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ВИДЫ СОБЫТИЙ БЕЗОПАСНОСТИ

Узловые средства защиты информации (далее – СЗИ) могут быть классифицированы следующим образом [6, 7].

- Средства (системы) защиты информации от несанкционированного доступа (СЗИ НСД). Обеспечивают реализацию моделей доступа субъектов к объектам, а также формируют журналы событий, базирующиеся на аудите доступа.
- Антивирусные программы, средства антивирусной защиты информации (САВЗ). Осуществляют поиск вредоносного программного обеспечения.
- Узловые системы обнаружения и предотвращения вторжений (HIDS/HIPS). Осуществляют контроль работы приложений.
- Средства защиты конечных устройств (EPP). Осуществляют поиск вредоносной активности на конечных устройствах.
- Системы автоматического выявления и устранения вредоносной активности на конечных устройствах (EDR). Осуществляют поиск вредоносной активности на конечных устройствах и блокирование этой активности.
- Системы контроля целостности (СКЦ). Осуществляют контроль целостности реестра, конфигурационных файлов и пользовательских файлов.
- Системы предотвращения утечек информации (DLP). Отслеживают перемещение конфиденциальной информации внутри и за пределами конечных устройств.

Каждый из СЗИ может генерировать события информационной безопасности в различных форматах [8]:

– общедоступных, например syslog или базы данных;

– проприетарных.

Каждый тип СЗИ генерирует уникальный набор событий безопасности, который может включать следующую информацию [9, 10]:

– об активности файловой системы: регистрация изменений файлов, состава файлов, реестра, временные метки, команды и/или командлеты терминалов;

– об активности системы идентификации и аутентификации: попытки несанкционированного доступа, угадывание или перебор паролей;

– о журналах событий;

– об активности в оперативной памяти;

– о планировщиков задач;
– о статистике используемых ресурсов;
– о вредоносных программах: обнаруженные вирусы, трояны, черви.

Основными способами передачи информации от узловых средств защиты информации являются:

– стандарты отправки и регистрации сообщений syslog;
– инструментарий управления Windows (WMI);
– базы данных;
– протоколы сетевого обмена файлами FTP или SMB;
– протоколы передачи гипертекстов HTTP или HTTPs.

Таким образом, каждое узловое СЗИ W_i по умолчанию можно описать кортежем (последовательностью):

$$W_i = \langle D, S \rangle, \tag{1}$$

где i – тип сетевого средства защиты информации (1 – СЗИ НСД, 2 – САВЗ, 3 – HIDS/HIPS, 4 – EPP/EDR, 5 – СКЦ, 6 – DLP); D – набор форматов данных для выгрузки событий информационной безопасности; S – события информационной безопасности.

Набор форматов данных D можно представить в виде

$$D = \{d_1, d_2, ..., d_l\}, \tag{2}$$

где l – количество форматов данных.

В свою очередь, системы мониторинга событий информационной безопасности R_j можно описать в виде кортежа:

$$R_j = \langle D, P \rangle, \tag{3}$$

где j – конкретный вендор системы мониторинга событий информационной безопасности (в данном исследовании не будут классифицироваться и уточняться все виды систем мониторинга); D – набор форматов данных для загрузки событий информационной безопасности (формально тот же самый показатель, что и для кортежа W_i); P – совместимость системы мониторинга с различными видами сетевых средств защиты информации.

2. МОДЕЛИ РАСПРОСТРАНЕНИЯ ПОСЛЕДСТВИЙ РЕАЛИЗАЦИИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

При анализе последствий компьютерного инцидента используются различные модели, которые помогают понять и предсказать, как инцидент может повлиять на информационные системы и организацию в целом [11–13]. Эти модели основываются на различных подходах и методах анализа, предоставляя структуру для оценки и управления последствиями инцидента.

Модель цепной реакции предполагает, что последствия компьютерного инцидента распространяются по системе подобно цепной реакции. В этой модели инцидент, затрагивающий один компонент системы, может последовательно привести к сбоям или нарушениям в других связанных компонентах. Например, атака на сервер базы данных может вызвать проблемы с доступом к данным, что, в свою очередь, нарушит работу приложений, зависящих от этой базы. Задача этой модели – идентифицировать и модулировать возможные «слабые звенья» в системе, чтобы минимизировать риск широкого распространения последствий инцидента. Такая модель распространения характерна для атак, нацеленных на захват злоумышленником определенных критичных узлов в сети: файловых хранилищ, контроллеров домена, веб-серверов и проч.

Каскадная модель распространения рассматривает инциденты, последствия которых распространяются по системе через цепочку зависимостей. В отличие от модели цепной реакции, которая может охватывать любые связанные компоненты, каскадная модель акцентируется на зависимостях между узлами. Например, если один узел в распределенной сети подвергся атаке и вышел из строя, каскадный эффект может привести к отключению других узлов, которые зависели от пострадавшего узла для выполнения своих функций. Эта модель помогает выявлять критические зависимости и узлы в системе, где сбои могут иметь наиболее значительные последствия. Такая модель характерна для атак, направленных на нарушение работоспособности центральных узлов серверного оборудования, например захват среды виртуализации, в которой размещены все основные активы для распределенных информационных систем. В таком случае потенциальный ущерб выше, чем у атак с цепной реакцией, в силу того, что нарушается работоспособность основных систем.

Модель вирусного распространения схожа с биологическими моделями распространения вирусов и акцентируется на том, как вредоносное ПО может быстро и широко распространяться по системам и сетям. В этой модели, как

только один узел (например, компьютер или сервер) становится инфицированным, он способен передавать вредоносное ПО другим узлам через сеть. Анализируя эту модель, специалисты по безопасности могут разрабатывать стратегии быстрого реагирования, чтобы изолировать инфицированные узлы и предотвратить распространение угрозы. Эта модель особенно важна для понимания и борьбы с эпидемиями компьютерных вирусов и червей. Такая модель характерна для большинства вредоносного программного обеспечения, целью которых является заражение как можно большего числа устройств в сети.

Авторы считают перспективным направлением использование моделирования информационных систем, в частности цифровых двойников [14, 15], для повышения информационной защищенности реальных систем, оценки эффективности узловых средств защиты информации как источников событий, а также оптимизации их структуры, так как они позволяют получить оценку поведения информационной системы, в том числе системы защиты информации в ситуациях, определяемых моделями распространения последствий реализации компьютерных инцидентов.

Цифровые двойники предоставляют доступ для исследования критически важных компонентов защищаемой системы, поведение которых можно исследовать на различных сценариях кибератак и распространения последствий реализации компьютерных инцидентов. Это позволяет оценить возможные последствия таких атак, выявлять уязвимые места и разрабатывать стратегии защиты без риска нарушения работоспособности реальной системы. Для решения задачи анализа последствий компьютерного инцидента в граничных условиях конкретной компьютерной сети критически важно иметь доступ к историческим и текущим данным о событиях, в том числе о событиях информационной безопасности, реальной сети.

Использование узловых средств защиты информации является ключевым элементом в противодействии распространению последствий компьютерных инцидентов, описываемых различными моделями. Благодаря своей способности обеспечивать безопасность на уровне отдельных компонентов системы данные средства становятся важным звеном в комплексной стратегии защиты информации и минимизации рисков, связанных с инцидентами, а также ценным источником данных для моделирования и систем мониторинга информационной безопасности.

3. КРИТЕРИИ ОЦЕНКИ ЭФФЕКТИВНОСТИ УЗЛОВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ КАК ИСТОЧНИКОВ СОБЫТИЯ ДЛЯ СИСТЕМ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Эффективность узловых средств защиты информации в рамках процесса мониторинга событий информационной безопасности [16] заключается в следующих возможностях:

1) выступать источником событий для систем мониторинга событий информационной безопасности (совместимость выгружаемого формата данных из узловых средств защиты информации с принимаемыми форматами данных систем мониторинга);

2) выявлять определенные техники и тактики злоумышленников;

3) выявлять компьютерные атаки и инциденты определенной модели распространения последствий компьютерных инцидентов;

4) самостоятельно осуществлять корреляцию событий для формирования уведомления о потенциальном компьютерном инциденте.

Таким образом, дополним описание сетевых средств защиты информации в формуле (1) новыми критериями:

$$W_i = \langle D, S, T, TA, M, K \rangle, \tag{4}$$

где T – набор детектируемых техник злоумышленников; TA – набор детектируемых стадий цепочки атак; M – набор детектируемых моделей распространения последствий компьютерных инцидентов; K – способность самостоятельной корреляции событий ИБ.

Ниже разберем каждый показатель.

Набор детектируемых техник злоумышленников можно представить так:

$$T = \{T_1, T_2, ..., T_n\}, \tag{5}$$

где n – количество техник злоумышленников,

Набор детектируемых тактик злоумышленников можно представить так:

$$TA = \{TA_1, TA_2, ..., TA_k\}, \tag{6}$$

где k – количество детектируемых стадий цепочки атак.

Набор детектируемых моделей распространения последствий компьютерных инцидентов можно представить так:

$$M = \{m_1, m_2, m_3\}, \tag{7}$$

где m_1 – модель распространения последствий компьютерных инцидентов типа цепная реакция; m_2 – модель распространения последствий компьютерных инцидентов типа каскад; m_3 – модель распространения последствий компьютерных инцидентов типа вирус.

Способность к корреляции событий информационной безопасности можно представить в виде

$$K = \begin{cases} 0 & \text{при отсутствие корреляции,} \\ 1 & \text{при присутствие корреляции.} \end{cases} \quad (8)$$

То есть при $K = 0$ необходимо применять функционал систем мониторинга событий информационной безопасности для проведения процедуры корреляции событий ИБ, а при $K = 1$ на системы мониторинга поступают уже скорелированные события.

Показатели D и S зависят от конкретного поставщика узловых средств защиты информации, а применимость их зависит от конкретного поставщика систем мониторинга событий информационной безопасности. В данном исследовании примем, что используемые средства защиты информации и системы мониторинга совместимы в рамках передачи, приема и обработки событий информационной безопасности, и сосредоточимся на остальных показателях. Таким образом, расчет показателя эффективности E узловых средств защиты информации выполняется сравнением показателей T, TA, M, K между разными узловыми средствами защиты информации по мощности соответствующих множеств:

$$E = \{|T|, |TA|, |M|, |K|\}. \quad (9)$$

Совместно с показателем эффективности проводится определение показателя совместимости F на основе показателя D между конкретным средством защиты информации и системой мониторинга событий для выявления совместимости:

$$F = \begin{cases} 0, D_w \cap D_R = \varnothing \vee W_i \notin P_R, \\ 1, D_w \cap D_R \neq \varnothing \wedge W_i \in P_R. \end{cases} \quad (10)$$

Таким образом, при оценке эффективности узловых средств защиты информации в рамках процесса мониторинга событий безопасности информационных систем проводится оценка двух показателей: совместимости средства защиты информации и системы мониторинга и непосредственно оценка

эффективности. В настоящем исследовании примем, что средства защиты информации и системы мониторинга совместимы между собой, а также поддерживаются все форматы данных для передачи событий безопасности.

4. АНАЛИЗ ЭФФЕКТИВНОСТИ УЗЛОВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ КАК ИСТОЧНИКОВ СОБЫТИЯ ДЛЯ СИСТЕМ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Соответствие между изучаемыми узловыми средствами защиты информации и детектируемыми ими техниками, тактиками и моделями распространения последствий компьютерных инцидентов представлено в таблице. Таблица сформирована на основании данных Mitre Attack: показатели *T* и *TA* являются ссылками на техники и тактики согласно классификации Mitre Attack.

Показатели эффективности узловых средств защиты информации как источников событий безопасности информации

Indicators of the effectiveness of central information security tools as sources of information security events

W	*T*	*TA*	*M*	*K*	*E*
1	1087.002, 1583.001, 1583.004, 1583.006, 1071.001, 1560.001, 1547.001, 1110, 1059.001, 1059.005, 1059.003, 1584.001, 1584.004, 1005, 1622, 1587.001, 1587.002, 1573.001, 1585.001, 1585.002, 1041, 1567.002, 1083, 1589, 1591.004, 1656, 1070.004, 1105, 1534, 1036.008, 1106, 1027.002, 1027.013, 1566.001, 1566.002, 1566.003, 1053.005, 1593.001, 1505.004, 1608.001, 1608.002, 1553.002, 1218.010, 1218.011, 1614.001, 1221, 1204.001, 1204.002, 1497.001, 1497.003, 1047, 1220, 1098, 1098.001, 1557, 1557.001, 1612, 1613, 1136, 1136.002, 1136.003, 1602, 1602.001, 1602.002, 1565, 1565.003, 1610, 1482, 1190, 1210, 1133, 1046, 1040, 1095, 1571, 1563, 1563.002, 1489, 1072, 1199, 1552.007, 0800, 0830, 0806, 0858, 0868, 0816, 0838, 0839, 0861, 0843, 0845, 0886, 0848, 0856, 0857, 0855, 0860	0001, 0002, 0003, 0004, 0005, 0006, 0007, 0008, 0009, 0010, 0040	1, 2	1	{98,11,2,1}

Продолжение таблицы
Continuation of the Table

W	*T*	*TA*	*M*	*K*	*E*
2	1566.002, 1204.001, 1204.002, 1664, 1660, 0865, 0864, 0863, 1547.006, 1059, 1059.001, 1059.005, 1059.006, 1564, 1564.012, 1036, 1036.008, 1027, 1027.002, 1027.009, 1027.010, 1027.012, 1027.013, 1566, 1566.001, 1566.003, 1221, 1080	0002, 0005, 0006, 0007, 0009, 0010, 0040	1, 2, 3	1	{28,7,3,1}
3	1040, 1057, 1518.001, 1007, 1553, T1553.004, 1562, 1562.001, 1070, 1070.009, 0872, 1112, 1548, 1548.002, 1557, 1557.001, 0830, 1547, 1547.001, 1547.002, 1547.003, 1547.004, 1547.005, 1547.010, 1547.012, 1547.014, 1543, 1543.003, 1074. 1074.001, 1546.001, 1546.002, 1546.007, 1546.008, 1546.009, 1546.010, 1546.011, 1546.012, 1546.015, 1564, 1564.002, 1564.005, 1564.006, 1574, 1574.007, 1574.011, 1574.012, 1562, 1562.001, 1562.002, 1562.004, 1562.006, 1562.009, 1070, 1070.007, 1070.009, 0872, 1490, 1056, 1056.001, 1556, 1556.002, 1556.008, 1112, 1111, 1137, 1137.001, 1137.002, 1137.006, 1003.001, 1505.005, 1489, 0881, 0856, 1553, 1553.003, 1553.004, 1553.006, 1218, 1218.002, 1569, 1569.002	0001, 0002, 0003, 0004, 0005, 0006, 0007, 0008, 0009	1, 2	1	{82,9,2,1}
4	1219, 1007, 1562.001, 1562.009, 1518.001, 0847, 1012, 1562, 1652, 1003, 1003.002, 1003.004, 1012, 1649, 1614.001, 1033, 1552, 1552.002, 1547, 1547.001, 1547.014, 1037, 1037.001, 1176, 1543, 1543.003, 1562.002, 1562.009, 1112, 1556, 1556.008, 1027, 1027.011, 1137, 1137.001, 1137.002, 1137.006, 1053.005	0001, 0002, 0003, 0004, 0005, 0006, 0007, 0008, 0009, 0010, 0040	1, 2	1	{38,11,2,1}

Окончание таблицы
End of the Table

W	*T*	*TA*	*M*	*K*	*E*
5	1098, 1098.002, 1098.005, 0800, 1557, 1557.003, 0830, 0803, 0804, 0805, 1110, 1110.001, 1110.002, 1110.003, 1110.004, 0806, 0858, 0807, 1213, 1213.001, 1213.002, 1213.003, 0811, 1622, 1491, 1491.001, 1491.002, 0814, 1610, 0816, 1484, 1484.002, 1189, 0817, 1114, 1114.002, 1114.003, 1499, 1499.002, 1499.003, 1499.004, 1048, 1567, 1567.004, 1190, 0819, 1203, 1212, 1211, 0820, 0890, 1210, 0866, 1133, 0822, 1657, 1200, 1564, 1564.008, 1562.002, 1656, 1070, 1070.008, 1534, 0838, 1556, 1556.006, 1556.007, 0821, 0836, 0889, 0839, 0801, 1621, 1027.005, 1137, 1137.003, 1137.004. 1137.005, 1069, 1069.003, 1566, 1566.001, 1566.002, 1566.003, 1566.004. 1598, 1598.001, 1598.002, 1598.003, 1598.004, 0861, 0843, 0845, 0848, 1594, 1505, 1505.001, 1505.002, 1505.003, 1648, 1072, 0865, 1649, 0857, 1537, 0864, 1199, 0855, 1552, 1552.008, 1550, 1550.004, 1204, 1204.003, 0863, 0860	0005, 0003, 0004, 0007, 0040	1, 2	1	{117,5,2,1}
6	0893, 0830, 0802, 0811, 0893, 0861, 0882, 0879, 0813, 0815, 0826, 0827, 0828, 0837, 0832, 1005, 1025, 1048, 1041, 1052, 1567, 1537, 0882, 0893	0010, 0009, 0040	1, 2	1	{24,3,2,1}

При анализе данных таблицы можно сделать ряд выводов:

1) как видно по показателю *K*, все средства защиты информации оснащены функционалом, позволяющим выполнять встроенную корреляцию событий (везде $K = 1$), что означает их способность не просто фиксировать и анализировать отдельные события в системе, но и выявлять взаимосвязи между ними;

2) все современные СЗИ также предоставляют средства защиты от моделей распространения последствий компьютерных атак, таких как цепные

реакции и каскады; согласно таблице все СЗИ соответствуют показателям m_1 и m_2;

3) антивирусные программы играют критически важную роль в защите от вирусной модели распространения последствий компьютерных инцидентов: только антивирусы могут детектировать атаки и инциденты, принадлежащие модели m_3;

4) СЗИ НСД, узловые IDS/IPS и EPP/EDR охватывают самый широкий спектр техник и тактик злоумышленников согласно показателям *T* и *TA* таблицы.

5. РЕКОМЕНДАЦИИ ПО ВЫБОРУ УЗЛОВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Для построения эффективной сети источников данных об инцидентах информационной безопасности рекомендуется интегрировать несколько уровней защиты, которые обеспечат комплексный подход к обнаружению и предотвращению различных типов угроз.

Во-первых, необходимо использовать антивирусное программное обеспечение для первичной защиты и мониторинга вредоносных программ. Антивирусы играют важную роль в выявлении и блокировке распространенных угроз, таких как вирусы и трояны, а кроме того, являются важным элементом подсистемы контроля используемого программного обеспечения.

Во-вторых, стоит включить в сеть источников СЗИ НСД и системы контроля целостности. Эти средства позволяют следить за конфигурациями систем, выявлять подозрительные изменения и обеспечивать защиту данных от неправомерного использования.

В-третьих, важную роль играют узловые IDS/IPS, которые отслеживают сетевой трафик, обнаруживают аномальные активности и предотвращают сложные атаки, такие как эксплуатация уязвимостей или атаки нулевого дня. Для еще более глубокого контроля следует применять решения уровня EPP и EDR, которые способны не только выявлять угрозы, но и реагировать на них в реальном времени. Наконец, интеграция систем предотвращения утечек данных (DLP) позволит обеспечить контроль за конфиденциальной информацией, предотвращая ее несанкционированное распространение.

Межсетевые экраны, в частности Web Application Firewall (WAF), играют важную роль в сети источников данных, предоставляя критически важную информацию о попытках проникновения и аномальной активности. Брандмауэры фильтруют трафик на периметре сети, блокируя

несанкционированные подключения и записывая все попытки взлома. Эти журналы событий становятся ценным источником данных для анализа угроз и помогают в построении профилей атак. В свою очередь, WAF защищает веб-приложения от угроз уровня приложений, таких как SQL-инъекции или межсайтовый скриптинг, и предоставляет информацию о характере и источнике этих атак.

ЗАКЛЮЧЕНИЕ

В условиях постоянного усложнения киберугроз и увеличения числа компьютерных инцидентов разработка объективной методики для оценки эффективности узловых средств защиты информации становится критически важной задачей. Основой такой методики служит учет различных моделей распространения последствий реализации компьютерных инцидентов, что позволяет адекватно оценивать способность СЗИ противостоять современным угрозам. Особое внимание уделяется анализу реакций системы на инциденты, а также устойчивости к многоступенчатым и комплексным атакам, характерным для каскадных и цепных моделей. Таким образом, формируется целостное видение того, насколько узловые СЗИ способны обеспечить гибкую и надежную защиту в условиях динамичных угроз.

Сформированная методика базируется на детальном изучении техник и тактик злоумышленников, что является основой для понимания механизма распространения атак и их последствий. Благодаря такому подходу методика не только оценивает существующие методы защиты, но и выявляет избыточные аспекты информационной безопасности, тем самым способствуя оптимизации и улучшению системы защиты.

Основная задача предлагаемой методики заключается в формировании наиболее эффективной защиты за счет устранения избыточных событий информационной безопасности, которые могут привести к ложным срабатываниям и перегрузке систем мониторинга. Анализируя моделирование угроз и техники атак, методика предлагает пути оптимизации существующих СЗИ с акцентом на их реакцию на реальные инциденты. Это достигается путем сокращения избыточных предупреждений и повышения точности идентификации вредоносных действий, что приводит к более рациональному использованию ресурсов безопасности и минимизации операционной нагрузки на команды по защиты информации.

В рамках разработанной методики сформированы рекомендации по применению существующих типов узловых СЗИ в зависимости от специфических условий и угроз, характерных для различных организаций. Эти рекомендации

включают подбор оптимальных конфигураций узловых средств защиты в зависимости от идентифицированных моделей угроз и характерных сценариев атак.

СПИСОК ЛИТЕРАТУРЫ

1. *Гончаренко С.Н., Лачихина А.Б.* Мониторинг инцидентов безопасности геоинформационной системы управления и контроля деятельности промышленного предприятия // Горный информационно-аналитический бюллетень. – 2022. – № 3. – С. 108–116.

2. *Ivanov S.O., Ilyin D.V., Ilyina L.A.* An optimal set of information security tools // European Proceedings of Social and Behavioural Sciences. – Prague, 2021. – Vol. 103: Finance, entrepreneurship and technologies in digital economy. – P. 479–484.

3. *Исхаков А.Ю.*, *Исхаков С.Ю.* Повышение эффективности систем защиты информации с помощью категоризации событий безопасности // Информационные и математические технологии в науке и управлении. – 2023. – № 2 (30). – С. 152–164.

4. *Condolo C.*, *Romero S.*, *Ticona W.* Implementation of an information security management system to improve the IT security of an agricultural tool manufacturing company // 2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India. – IEEE, 2024. – P. 177–183.

5. *Karimov M.M., Arzieva J.T., Rakhimberdiev K.* Development of approaches and schemes for proactive information protection in computer networks // 2022 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan. – IEEE, 2022. – P. 1–5.

6. System-level data management for endpoint advanced persistent threat detection: issues, challenges and trends / T. Chen, C. Zheng, T. Zhu, C. Xiong, J. Ying, Q. Yuan, W. Cheng, M. Lv // Computers & Security. – 2023. – Vol. 135. – P. 103485.

7. *Adu-Kyere A., Nigussie E., Isoaho J.* Analyzing the effectiveness of IDS/IPS in real-time with a custom in-vehicle design // Procedia Computer Science. – 2024. – Vol. 238. – P. 175–183.

8. Knock, knock, log: threat analysis, detection & mitigation of covert channels in syslog using port scans as cover / K. Lamshöft, T. Neubert, J. Hielscher, C. Vielhauer, J. Dittmann // Forensic Science International: Digital Investigation. – 2022. – Vol. 40. – P. 301335.

9. *Alahmadi A., Alkhraan N., BinSaeedan W.* MPSAutodetect: a malicious PowerShell script detection model based on stacked denoising auto-encoder // Computers & Security. – 2022. – Vol. 116. – P. 102658.

10. *Yan S.-H., Ku C.C.-Y.* Using language-specific input methods and pronunciation rules to improve the guesses of passwords // Journal of Information Security and Applications. – 2023. – Vol. 77. – P. 103588.

11. *Маликов А.В., Авраменко В.С., Саенко И.Б.* Модель и метод диагностирования компьютерных инцидентов в информационно-коммуникационных системах, основанные на глубоком машинном обучении // Информационно-управляющие системы. – 2019. – № 6. – С. 32–42.

12. Enterprise architecture modeling for cybersecurity analysis in critical infrastructures – A systematic literature review / Y. Jiang, M.A. Jeusfeld, M. Mosaad, N. Oo // International Journal of Critical Infrastructure Protection. – 2024. – Vol. 46. – P. 100700.

13. *Negrea Petru-Cristian*. A comprehensive analysis of high-impact cybersecurity incidents: case studies and implications: Master Thesis / Babeș–Bolyai University. – Cluj-Napoca, 2024. – 121 p.

14. Цифровые двойники: вопросы терминологии: обзор / А.И. Боровков, Ю.А. Рябов, Л.А. Щербина, А.А. Гамзикова. – СПб.: Политех-Пресс, 2021. – 25 с.

15. A perfect storm: digital twins, cybersecurity, and general contracting firms / E. Pärn, N. Ghadiminia, B. García de Soto, K. Oti-Sarpong // Developments in the Built Environment. – 2024. – Vol. 18. – P. 100466.

16. Оценка функционирования SIEM-систем на основе комплекса критериев эффективности / М.М. Путято, А.С. Макарян, А.Н. Черкасов, В.А. Кучер // Вестник Адыгейского государственного университета. Серия 4, Естественно-математические и технические науки. – 2024. – № 1 (336). – С. 36–42.

Марченко Михаил Александрович, директор лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики СО РАН. Основное направление научных исследований – математическое моделирование, цифровые двойники. E-mail: marchenko@sscc.ru

Пермяков Руслан Анатольевич, ведущий инженер лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики СО РАН. Область научных интересов: цифровые двойники в области информационной безопасности, защита информации объектов научного назначения. E-mail: pra@sscc.ru

Огнев Игорь Александрович, инженер лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики СО РАН. Область научных интересов: имитационное моделирование в области информационной безопасности, защита информации объектов научного назначения. E-mail: ognev.igor.alex@gmail.com

Никрошкин Иван Владимирович, инженер лаборатории искусственного интеллекта и информационных технологий Института вычислительной математики и математической геофизики СО РАН. Область научных интересов: мониторинг событий безопасности информационных систем, защита информации объектов научного назначения. E-mail: ivan.nikroshkin@bk.ru

DOI: 10.17212/2782-2230-2024-4-84-102

Issues of collecting information about security events from host information security tools as part of security monitoring*

M.A. Marchenko[1], R.A. Permyakov[2], I.A. Ognev[3], I.V. Nikroshkin[4]

[1] *Institute of Computational Mathematics and Mathematical Geophysics, Siberian Branch of the Russian Academy of Sciences, 6 Academician Lavrentyev Avenue, Novosibirsk, 630090, Russian Federation, PhD of Physical and Mathematical Sciences, Professor of the Russian Academy of Sciences, director of the Laboratory of Artificial Intelligence and Information Technologies. E-mail: marchenko@sscc.ru*

[2] *Institute of Computational Mathematics and Mathematical Geophysics, Siberian Branch of the Russian Academy of Sciences, 6 Academician Lavrentyev Avenue, Novosibirsk, 630090, Russian Federation, leading engineer of the Laboratory of Artificial Intelligence and Information Technologies. E-mail: pra@sscc.ru*

[3] *Institute of Computational Mathematics and Mathematical Geophysics, Siberian Branch of the Russian Academy of Sciences, 6 Academician Lavrentyev Avenue, Novosibirsk, 630090, Russian Federation, engineer of the Laboratory of Artificial Intelligence and Information Technologies. E-mail: ognev.igor.alex@gmail.com*

[4] *Institute of Computational Mathematics and Mathematical Geophysics, Siberian Branch of the Russian Academy of Sciences, 6 Academician Lavrentyev Avenue, Novosibirsk, 630090, Russian Federation, engineer of the Laboratory of Artificial Intelligence and Information Technologies. E-mail: ivan.nikroshkin@bk.ru*

Currently, the role of the process of monitoring security events in information systems, including distributed information systems, is growing. Information security tools, including nodal information security tools, are the main sources of information security events for security

* *Received 02 December 2024.*

The work was carried out according to the state assignment of the ICM&MG SB RAS (topic No. FSFWNM-2022-0005).

monitoring systems. Not all nodal information security tools presented today are equally useful and informative as sources of information security events for monitoring systems. This study raises issues of assessing the effectiveness of nodal information security tools as sources of information security events. The proposed assessment of effectiveness is based on the analysis of the ability of nodal information security tools to detect various models of spreading the consequences of computer incidents, as well as on the ability to detect certain techniques and tactics of intruders, which they use to implement computer attacks that entail computer incidents. The following nodal means of information protection were considered within the framework of this study: information protection systems against unauthorized access, anti-virus information protection means, nodal systems for detection and prevention of intrusions, end device protection means, systems for automatic detection and elimination of malicious activity on end devices, integrity control systems, information leakage prevention systems. The formed assessment of the effectiveness of nodal means of information protection as sources of security events allows implementing a more effective information protection system and the process of monitoring security events by eliminating redundant information security events that can lead to false alarms and overload of monitoring systems. In addition, based on the methodology and analysis of existing types of nodal means of information protection, recommendations were formed aimed at increasing the level of protection of the information infrastructure of organizations, which contributes to the creation of a more adaptive and dynamic system of counteracting threats.

Keywords: information security tools, host information security tools, efficiency, monitoring, security monitoring, information security, cybersecurity, models of spreading the consequences of computer incidents

REFERENCES

1. Goncharenko S.N., Lachihina A.B. Monitoring intsidentov bezopasnosti geoinformatsionnoi sistemy upravleniya i kontrolya deyatel'nosti promyshlennogo predpriyatiya [Monitoring of geoinformation system security incidents in performance supervision and management in industry]. *Gornyi informatsionno-analiticheskii byulleten' = Mining information and analytical bulletin*, 2022, no. 3, pp. 108–116.

2. Ivanov S.O., Ilyin D.V., Ilyina L.A. An optimal set of information security tools. *European Proceedings of Social and Behavioural Sciences*. Prague, 2021, vol. 103. *Finance, entrepreneurship and technologies in digital economy*, pp. 479–484.

3. Iskhakov A.Yu., Iskhakov S.Yu. Povyshenie effektivnosti sistem zashchity informatsii s pomoshch'yu kategorizatsii sobytii bezopasnosti [Improving the efficiency of information protection systems by categorizing security events]. *Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii = Information and Mathematical Technologies in Science and Management*, 2023, no. 2 (30), pp. 152–164.

4. Condolo C., Romero S., Ticona W. Implementation of an information security management system to improve the IT security of an agricultural tool manufacturing company. *2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2024, pp. 177–183.

5. Karimov M.M., Arzieva J.T., Rakhimberdiev K. Development of approaches and schemes for proactive information protection in computer networks. *2022 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, Uzbekistan, 2022, pp. 1–5.

6. Chen T., Zheng C., Zhu T., Xiong C., Ying J., Yuan Q., Cheng W., Lv M. System-level data management for endpoint advanced persistent threat detection: issues, challenges and trends. *Computers & Security*, 2023, vol. 135, p. 103485.

7. Adu-Kyere A., Nigussie E., Isoaho J. Analyzing the effectiveness of IDS/IPS in real-time with a custom in-vehicle design. *Procedia Computer Science*, 2024, vol. 238, pp. 175–183.

8. Lamshöft K., Neubert T., Hielscher J., Vielhauer C., Dittmann J. Knock, knock, log: threat analysis, detection & mitigation of covert channels in syslog using port scans as cover. *Forensic Science International: Digital Investigation*, 2022, vol. 40, p. 301335.

9. Alahmadi A., Alkhraan N., BinSaeedan W. MPSAutodetect: a malicious PowerShell script detection model based on stacked denoising auto-encoder. *Computers & Security*, 2022, vol. 116, p. 102658.

10. Yan S.-H., Ku C.C.-Y. Using language-specific input methods and pronunciation rules to improve the guesses of passwords. *Journal of Information Security and Applications*, 2023, vol. 77, p. 103588.

11. Malikov A.V., Avramenko V.S., Saenko I.B. Model' i metod diagnostirovaniya komp'yuternykh intsidentov v informatsionno-kommunikatsionnykh sistemakh, osnovannye na glubokom mashinnom obuchenii [Model and method for diagnosing computer incidents in information and communication systems based on deep machine learning]. *Informatsionno-upravlyayushchie sistemy = Information and Control Systems*, 2019, no. 6, pp. 32–42.

12. Jiang Y., Jeusfeld M.A., Mosaad M., Oo N. Enterprise architecture modeling for cybersecurity analysis in critical infrastructures – A systematic literature review. *International Journal of Critical Infrastructure Protection*, 2024, vol. 46, p. 100700.

13. Negrea Petru-Cristian. *A comprehensive analysis of high-impact cybersecurity incidents: case studies and implications*. Master thesis. Babeș–Bolyai University. Cluj-Napoca, 2024. 121 p.

14. Borovkov A.I., Ryabov Yu.A., Shcherbina L.A., Gamzikova A.A. *Tsifrovye dvoiniki: voprosy terminologii:* obzor [Digital twins: issues of terminology: review]. St. Petersburg, Politekh-Press, 2021. 25 p.

15. Pärn E., Ghadiminia N., García de Soto B., Oti-Sarpong K. A perfect storm: digital twins, cybersecurity, and general contracting firms. *Developments in the Built Environment*, 2024, vol. 18, p. 100466.

16. Putyato M.M., Makaryan A.S., Cherkasov A.N., Kucher V.A. Otsenka funktsionirovaniya SIEM-sistem na osnove kompleksa kriteriev effektivnosti [Estimation of functioning of SIEM systems based on a developed set of effectiveness criteria]. *Vestnik Adygeiskogo gosudarstvennogo universiteta. Seriya 4, Estestvenno-matematicheskie i tekhnicheskie nauki = Bulletin of the Adyghe State University. Series: Natural, Mathematical and Technical Sciences*, 2024, no. 1 (336), pp. 36–42.

Для цитирования:

Вопросы сбора информации о событиях безопасности с узловых средств защиты информации в рамках осуществления мониторинга безопасности / М.А. Марченко, Р.А. Пермяков, И.А. Огнев, И.В. Никрошкин // Безопасность цифровых технологий. – 2024. – № 4 (115). – С. 84–102. – DOI: 10.17212/2782-2230-2024-4-84-102.

For citation:

Marchenko M.A., Permyakov R.A., Ognev I.A., Nikroshkin I.V. Voprosy sbora informatsii o sobytiyakh bezopasnosti s uzlovykh sredstv zashchity informatsii v ramkakh osushchestvleniya monitoringa bezopasnosti [Issues of collecting information about security events from host information security tools as part of security monitoring]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 4 (115), pp. 84–102. DOI: 10.17212/2782-2230-2024-4-84-102.