sistem. Bazovaya etalonnaya model. Chast 1. Bazovaya model [Moscow Research Center (MSIC) State Committee of the Russian Federation for Communications and Informatization. GOST R ISO/IEC 7498-1-99 Information technology. Open Systems Interconnection. Basic Reference Model. Part 1. The Basic Model]. *gostrf*, 2006. Available at: http://www.gostrf.com/normadata/1/4294818/4294818276.pdf (accessed 14.01.2021).

15. Zhukov R. Sravnenie servisov po zashchite ot DDoS-atak [Comparison of DDoS protection services]. *anti-malware*, 2019. Available at: https://www.anti-malware.ru/compare/DDoS-attack-protection-services (accessed 15.01.2021).

16. Podborka: 12 servisov dlya zashchity ot DDoS-atak [Selection: 12 services to protect against DDoS attacks]. *Habr*, 2018. Available at: https://habr.com/ru/post/350384/ (accessed 15.01.2021).

17. Putyato M. M., Makaryan A. S., Chich Sh. M., Markova V. K. Issledovanie primeneniya tekhnologii deception dlya predotvrashcheniya ugroz kiberbezopasnosti [Research On the Use of Deception Technology to Prevent Cybersecurity Threats]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, pp. 85–98.

DOI 10.21672/2074-1707.2021.53.1.074-082
УДК 004.051

ИССЛЕДОВАНИЕ IRP-СИСТЕМ НА ОСНОВЕ АНАЛИЗА МЕХАНИЗМОВ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья поступила в редакцию 15.01.2021, в окончательном варианте – 17.02.2021.

Очередько Андрей Романович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru

Бачманов Дмитрий Андреевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID:0000-0003-3474-6831, e-mail: bachmanov.dm@gmail.com

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com

Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru

В статье рассматриваются особенности и функции систем реагирования на инциденты информационной безопасности. Представлен анализ современных решений IRP и описан процесс реагирования на типовые инциденты в системах этого класса. На основании экспертных мнений сформирован перечень критериев, которые были распределены в группы по зонам функциональной ответственности для дальнейшего сравнения работы IRP-систем. Произведена оценка основных и дополнительных характеристик IRP-систем с использованием сформированных критериальных групп. Анализ результатов сравнения показал, что наиболее перспективными решениями являются R-Vision IRP, IBM Resilient IRP и open-source решение – The Hive. Разработан и представлен алгоритм модуля предотвращения фишинговых атак, программная реализация которого произведена с использованием языка Python. В рамках интеграционных возможностей системы The Hive реализована пользовательская функция реагирования, которая не только потенциально улучшила работу системы при предотвращении фишинговых атак, но и увеличила осведомленность сотрудников об этой угрозе. Результатом является IRP-система с персональной гибкой настройкой отдельных элементов и является основой при формировании Центра обеспечения безопасности (SOC), который позволит вывести информационную безопасность организаций на новый уровень.

Ключевые слова: кибербезопасность, IRP-системы, инцидент информационной безопасности, кибератака, механизмы реагирования на инциденты, фишинговые атаки

RESEARCH OF IRP SYSTEMS BASED ON THE ANALYSIS OF MECHANISMS OF RESPONSE TO INFORMATION SECURITY INCIDENTS

The article was received by the editorial board on 15.01.2021, in the final version – 17.02.2021.

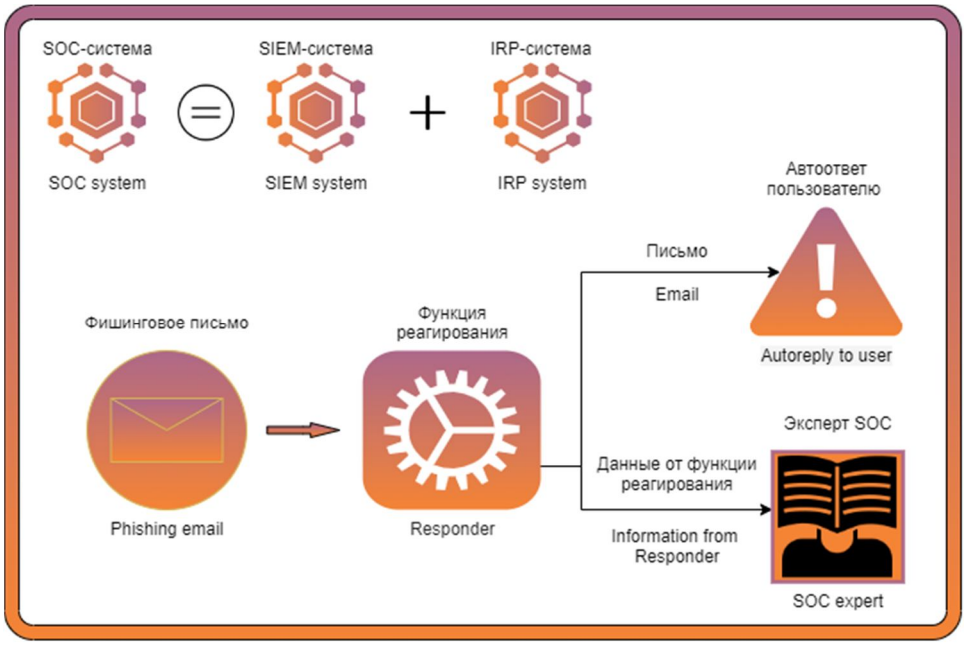
Ocheredko Andrey R., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
graduate student, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru

Bachmanov Dmitriy A., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
graduate student, ORCID: 0000-0003-3474-6831, e-mail: bachmanov.dm@gmail.com
Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru

The article discusses the features and functions of information security incident response systems. The analysis of modern IRP solutions is presented and the process of responding to typical incidents in systems of this class is described. Based on expert opinions, a list of criteria was formed, which were divided into groups by areas of functional responsibility for further comparison of the work of IRP systems. The assessment of the main and additional characteristics of IRP-systems was carried out using the formed criterion groups. The analysis of the comparison results showed that the most promising solutions are R-Vision IRP, IBM Resilient IRP and open-source solution - The Hive. The algorithm of the module for preventing phishing attacks was developed and presented, the software implementation of which was made using the Python language. As part of the integration capabilities of The Hive, a custom response function was implemented that not only potentially improved the system's performance in preventing phishing attacks, but also increased employee awareness of this threat. The result is an IRP system with personal flexible customization of individual elements and is the basis for the formation of the Security Center (SOC), which will bring the information security of organizations to a new level.

Keywords: cybersecurity, IRP systems, information security incident, cyber attack, incident response mechanisms, phishing attacks

Graphical annotation (Графическая аннотация)



Введение. В настоящее время информационные системы быстро развиваются, становятся обширнее и объединяют в себе множество подсистем для выполнения широкого спектра задач. С ростом количества и качества информационных систем развиваются и способы защиты информации от кибератак. Поиск решений, позволяющих минимизировать вред от нарушения информационной безопасности (ИБ), является актуальной задачей [1]. В этой работе мы рассмотрим совокупность возможных систем, средств и способов достижения приемлемого уровня защиты информационных активов современных организаций. Когда инфраструктура организации настолько сложна, что невозможно уследить за общей картиной происходящего, на помощь приходит Центр обеспечения безопасности (SOC, Security Operations Center) – это широко специализированный ситуационный центр мониторинга информационной безопасности, представляющий собой

совокупность программно-аппаратных средств, персонала и процессов [2]. Данный тип систем предназначен для централизованного сбора и анализа информации о событиях и инцидентах информационной безопасности (ИБ), поступающих из различных источников ИТ-инфраструктуры. Существует множество конкретных решений, но без ряда базовых средств мониторинга и защиты информации сложно себе представить даже внутренний SOC в средней компании («in-source»), не говоря уже о коммерческом центре. К таким средствам принято относить системы различного класса, где каждый элемент выполняет свою функциональную роль (рис. 1).

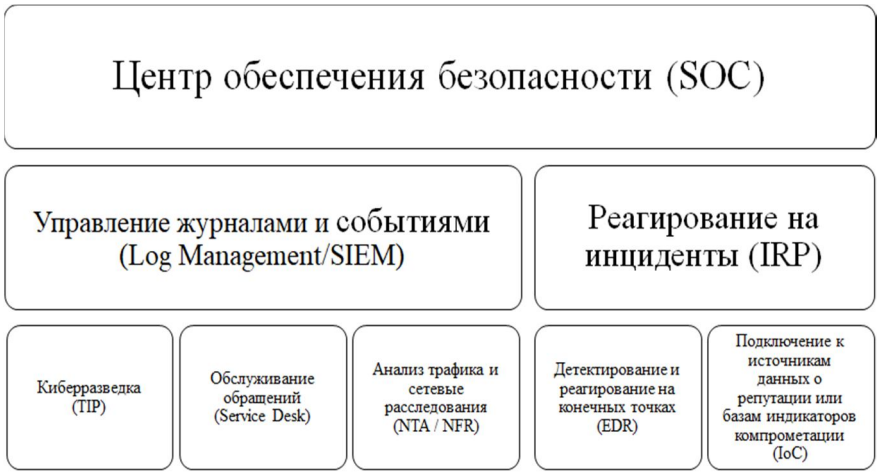


Рисунок 1 – Структура SOC

Особенности IRP систем. В предыдущих исследованиях был представлен анализ механизмов SIEM-систем и выбор лучшего решения с последующей его доработкой [3]. В данной статье мы остановимся на системе реагирования на инциденты (Incident Response Platforms, IRP) – отдельной системы для выстраивания процессов управления инцидентами, которая предназначена для автоматизации процессов мониторинга, учета и реагирования на инциденты информационной безопасности (ИБ) [4], а также решения типовых проблем управления ИБ (рис. 2) [5].

Рисунок 2 – Типы проблем управления ИБ

Поэтому применение IRP позволяет обеспечивать своевременные ответные действия группы реагирования на инциденты информационной безопасности, предоставляя при этом аналитическую информацию и контекст отслеживаемого события. Для эффективной работы IRP должна выполнять определенный перечень функций [6]:

- автоматизация процесса управления инцидентами ИБ;
- ведение единой базы знаний инцидентов;
- интеграция с существующими в компании средствами;
- совместная работа между группами реагирования на инциденты;
- автоматизация реагирования на инциденты;
- адаптивность работы;
- отчетность о проделанной работе;
- интеграция с внешними источниками.

Автоматизация процесса управления инцидентами ИБ является основной задачей IRP и предназначена для снижения нагрузки на персонал компании, связанный с обеспечением ИБ.

Ведение единой базы знаний инцидентов. Содержание в базе информации о зафиксированных инцидентах ИБ позволяет обеспечить регистрацию фактов выявления инцидентов в едином месте и повысить эффективность деятельности группы реагирования на инциденты.

Интеграция с существующими в компании средствами защиты посредством механизмов взаимодействия с целью объединения информации об инцидентах ИБ.

Совместная работа между группами реагирования на инциденты, а именно обеспечение механизмов коммуникации, оповещения о вновь появившихся инцидентах, хранения полученных материалов и его совместного анализа.

Автоматизация реагирования на инциденты. Вследствие того, что в некоторых случаях промежуток времени между обнаружением и реакцией на инцидент ИБ должен быть как можно меньше, необходимо как можно больше автоматизировать процесс реагирования на инциденты. Данные процедуры, как правило, включают готовые сценарии реагирования, совокупность технических мероприятий по обработке инцидента.

Адаптивность работы. Различие используемой инфраструктуры, средств защиты, процессов управления ИБ в различных компаниях порождает обеспечение адаптивности под группы реагирования на инциденты без участия поставщиков платформы.

Отчетность о проделанной работе. В связи с тем, что вопросы инцидентов ИБ рассматриваются руководством компании, регуляторами и контрагентами, существует необходимость визуализации полученной информации в виде диаграмм, наглядных графиков и карт, а также реализации отчета, включающего всю информацию, затрагивающую инциденты ИБ.

Интеграция с внешними источниками. Основной задачей является взаимодействие с другими участниками отрасли, экспертами и внешними организациями, а также центром реагирования на компьютерные инциденты (CERT) с целью получения оперативной и актуальной информации для своевременного принятия защитных мер.

Представим функциональную схему работы IRP-системы при осуществлении процесса реагирования на инциденты информационной безопасности (рис. 3).

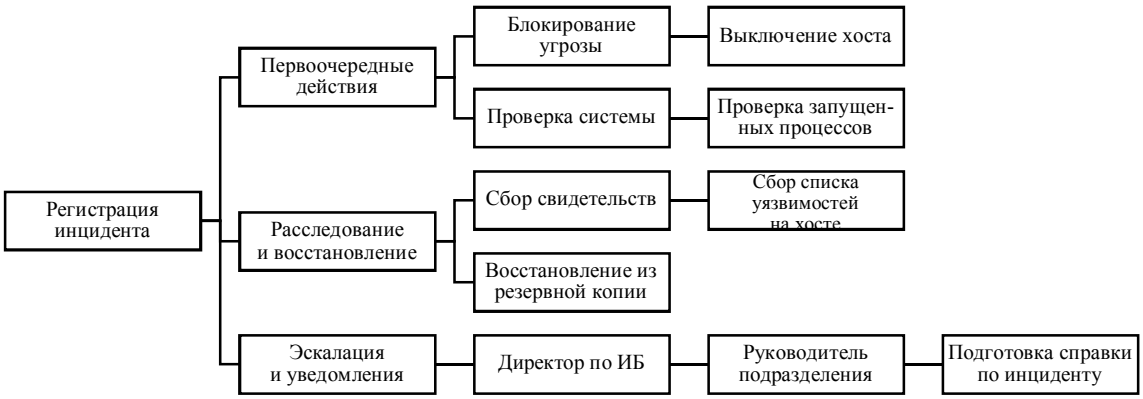


Рисунок 3 – Функциональная схема работы IRP в процессе реагирования на типовые инциденты ИБ

На данной схеме представлены основные этапы функционального взаимодействия в рамках работы с событием информационной безопасности. Эффективность работы системы в целом зависит от того, насколько точно, быстро и правильно отработает каждый блок. Так как производители являются прямыми конкурентами, каждый из них старается использовать инновационные решения при построении каркаса функционирования своей системы. Целесообразно использовать характеристики этих блоков при сравнении и анализе систем между собой.

Сравнение IRP-систем. Ведущими производителями представлено достаточно много решений в области IRP-систем, как коммерческих, так и свободного распространения:

- Jet Signal [7];
- R-Vision IRP [8];
- Security Vision IRP [9];
- IBM Resilient IRP [10];
- The Hive [11].

Проведем анализ использования программных решений IRP в SOC-системах. Для сравнения будем использовать перечень критериев, сформированный на основе исследований экспертного сообщества [12]. Объединим критерии в группы по зонам функциональной ответственности для дальнейшего сравнения работы IRP-систем:

1. Управление инцидентами – 30 %.
1.1. Карточка инцидентов.
1.2. Планирование и обработка инцидентов.
1.3. Автоматическое реагирование.
2. Управление уязвимостями – 30 %.
2.1. Настройка собственной модели определения критичных уязвимостей.
2.2. Авторегистрация уязвимостей.
2.3. Сортировка уязвимостей по критериям.
2.4. Возможность выделения ложных срабатываний.
3. Управление рисками – 25 %.
3.1. Карточка риска.
3.2. Оценка степени реализации угрозы и тяжести последствий.
3.3. Произвольные формулы расчета риска.
4. Интеграционные возможности системы – 15 %.
4.1. Интеграция с SIEM.
4.2. Интеграция со сканерами уязвимостей.
4.3. Интеграция с IPS.
4.4. Интеграция с DLP.

Каждая из групп имеет свою степень влияния, выраженную в процентном соотношении к общему объему возможностей системы. Произведем оценку характеристик IRP-систем, используя вышеописанные критериальные группы (табл.).

Таблица – Сравнение IRP-систем

№ п/п	Наименование критерия	Jet Signal	R-Vision IRP	Security Vision IRP	IBM Resilient IRP	The Hive
1.1	Карточка инцидентов	0,3	0,3	0,3	0,3	0,3
1.2	Планирование и обработка инцидентов	0,2	0,3	0,2	0,3	0,2
1.3	Автоматическое реагирование	0,3	0,3	0,3	0,3	0,3
2.1	Настройка собственной модели определения критичных уязвимостей	0,3	0,3	0,3	0,3	0,3
2.2	Настройка собственной модели определения критичных уязвимостей	0,3	0,3	0,3	0,3	0,3
2.3	Авторегистрация уязвимостей	0,3	0,3	0,3	0,3	0,3
2.4	Сортировка уязвимостей по критериям	0,2	0,1	0,1	0,1	0,3
3.1	Возможность выделения ложных срабатываний	0,2	0,3	0,3	0,3	0,3
3.2	Карточка риска	0,2	0,2	0,2	0,2	0,2
3.3	Оценка степени реализации угрозы и тяжести последствий	0,2	0,2	0,1	0,2	0,3
4.1	Произвольные формулы расчета риска	0,2	0,2	0,2	0,2	0,2
4.2	Интеграция со сканерами уязвимостей (vulnerability scanner)	0,2	0,2	0,2	0,2	0,2
4.3	Интеграция с IPS	0,2	0,2	0,2	0,2	0,2
4.4	Интеграция с DLP	0,2	0,2	0,2	0,2	0,1
Итог		3,3	3,4	3,2	3,4	3,5

Сравнение продуктов показывает, что наиболее подходящими при реализации дополнительных систем защиты от фишинговых атак являются приложения R-Vision IRP, IBM Resilient IRP и open-source-решение – The Hive.

Реализация защиты от фишинговых атак. Для реализации защиты выберем систему The Hive. Встроенный механизм пользовательских функций реагирования (Responder) может быть использован для помощи в программе повышения осведомленности пользователей путем создания автоматических ответов на случаи, связанные с фишингом.

Разработчики системы предоставили руководство для создания функций реагирования, которые подходят для реализации возможных способов решения задач защиты. В системе есть встроенная виртуальная машина, которая используется для написания собственных функций реагирования, она позволяет протестировать и настроить все, что является необходимым для собственной функции [13].

В рамках рассматриваемого примера необходимо упомянуть об особенностях фишинга в электронной почте. Фишинг – массовая рассылка электронных писем или сообщений для того, чтобы заманить пользователя на web-сайты, которые внешне очень похожи на обычные web-сайты различных фирм и банков, но контролируются мошенниками. В результате заранее продуманных действий электронные мошенники вынуждают пользователя оставлять на таком web-сайте нужные им конфиденциальные сведения о паролях, номерах кредитных карт, банковских счетов и прочее [14, 15]. В прогнозах на 2021 от компании Group-IB фишинг упоминается как серьезная проблема, злоумышленники используют гибридные фишинговые атаки с использованием социальной инженерии [16, 17]. В такой ситуации очень важно постоянно повышать осведомленность сотрудников, чтобы новые разновидности фишинга не смогли ввести в заблуждение работников организации [18].

Решением задачи является создание модифицированных функций реагирования на фишинговые атаки при помощи совокупности скриптов на языке Python и конфигурационных элементов, которые позволяют системе интерпретировать получаемые данные из внешних источников [19].

В нашем данном случае рассмотрим проявление фишинга в виде сообщений в корпоративной электронной почте организации. Такое проявление фишинга в корпоративной среде представляет собой тщательно продуманную и реализованную таргетированную атаку. Благодаря функции реагирования система сможет моментально получить определенные параметры, которые будут необходимы эксперту для создания полной картины инцидента [20]:

- почтовый адрес, от имени которого пришло письмо;
- SMTP-сервер, использованный для отправки письма;
- порт SMTP-сервера;
- пользователь SMTP-сервера;
- пароль от SMTP-сервера.

Для того чтобы создать и запустить функцию реагирования, необходимо подготовить 2 файла: конфигурационный файл JSON и Python-файл с кодом, в котором будет описана логика-функция.

Необходимые для заполнения параметры в JSON-файле конфигурации:

- DataTypeList – это поле указывает, применим ли ответчик к рабочему случаю (use case), оповещению (alert) или просто подозрительному случаю. Разница заключается во входных данных, которые передаются системы к ответчику. Скрипт будет получать структуру JSON, представляющую случай, предупреждение или подозрительный момент. В этом примере будет сделан ответчик, применимый к рабочим случаям (use case);
- Command – это путь к скрипту относительно папки Responders, в нашем примере кода: Phishing/phishing.py;
- Config – это поле позволяет определять разные «разновидности» одних и тех же ответчиков: в системе может быть один сценарий, который предоставляет несколько различных выводов, которые будут отображаться как разные ответчики;
- ConfigurationItems – данное поле является параметром типа DataSet или набор данных, оно определяет все параметры, которые должны быть установлены пользователями через графический интерфейс системы.

В файл с логикой работы функции мы будем закладывать те же параметры, которые использовали в конфигурационном файле в интерпретации языка Python. Построим блок-схему алгоритма (рис. 5).

Настройка пользовательских функций реагирования на новые классы инцидентов потенциально улучшает не только работу системы, но и повышает качество и развитость работы функциональных блоков при предотвращении фишинговых атак. Также при помощи функции были заданы автоматические ответы сотрудникам, которые дополнительно сообщили о подозрительных письмах, тем самым повысив осведомленность персонала об опасности фишинговых писем.

Рисунок 5 – Алгоритм работы Python-скрипта

Заключение. В результате проведенного исследования были выделены особенности и функции IRP-систем. Анализ современных решений IRP и мнений экспертов в области информационной безопасности позволил сформировать перечень критериев, которые были распределены в группы по зонам функциональной ответственности для дальнейшего сравнения работы IRP-систем. Произведена оценка характеристик IRP-систем с использованием сформированных критериальных групп. Анализ результатов сравнения показал, что наиболее перспективными решениями являются R-Vision IRP, IBM Resilient IRP и open-source-решение – The Hive. Приведен пример реализации пользовательской функции реагирования, которая не только потенциально улучшила работу системы при предотвращении фишинговых атак, но и позволила увеличить осведомленность сотрудников об этой угрозе. IRP-системы позволяют провести персональную настройку практически в любой ситуации и, как и SIEM-системы, являются основой при формировании Центра обеспечения безопасности (SOC) организации. Необходимо продолжать постоянное расширение и модернизацию функций IRP-систем для поддержания высокого уровня безопасности в условиях роста количества киберугроз. Благодаря политике свободного доступа к алгоритмам The Hive, мы будем продолжать исследования как в области модернизации существующих решений учета и реагирования инцидентов, так и в построении Центра обеспечения безопасности в целом.

Библиографический список

1. Путято М. М. Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства / М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 3. – С. 94–102.

2. Путято М. М. Адаптивная система комплексного обеспечения безопасности как элемент инфраструктуры ситуационного центра / М. М. Путято, А. С. Макарян, А. Н. Черкасов, И. В. Горин // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 4. – С. 75–84.

3. Очередько А. Р. Исследование SIEM-систем на основе анализа механизмов выявления кибератак / А. Р. Очередько, В. С. Герасименко, М. М. Путято, А. С. Макарян // Вестник АГУ. Серия 4: Естественно-математические и технические науки. – 2020. – № 2. – С. 25–31.

4. Сравнение систем SGRC (Security Governance, Risk, Compliance). – 2017. – Режим доступа: https://www.anti-malware.ru/compare/russian_sgrc_2017, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 04.01.2021).

5. Обзор рынка платформ реагирования на инциденты (IRP) в России. – 2018. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/incident-response-platforms-irp-in-russia, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 11.01.2021).

6. Бесплатная IRP-система своими силами: опыт использования платформы с открытым кодом The Hive. – 2019. – Режим доступа: https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

7. Система управления инцидентами информационной безопасности Jet Signal. – Режим доступа: https://jet.su/services/software-development/products/jet-signal/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

8. Платформа для создания Центра реагирования на инциденты ИБ. – Режим доступа: https://rvision.pro/irp/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

9. Системы класса Incident Response Platform: применение и основные функции. – Режим доступа: https://www.securityvision.ru/products/irp/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

10. Платформа координации и автоматизации процессов реагирования на инциденты. – Режим доступа: https://www.ibm.com/ru-ru/products/resilient-soar-platform, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

11. Security incident response for the masses. – Режим доступа: https://thehive-project.org/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

12. Системы реагирования и управления инцидентами информационной безопасности (IRP). – 2019. – Режим доступа: https://www.anti-malware.ru/security/irp, свободный.– Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

13. The Hive-Project. – 2020. – Режим доступа: https://github.com/TheHive-Project/TheHive, свободный. – Заглавие с экрана. – Яз.англ. (дата обращения: 05.01.2021).

14. Примеры фишинга через электронную почту: как распознать фишинговое письмо. – 2020. – Режим доступа: http://www.itsec.ru/articles/primery-fishinga-cherez-elektronnuyu-pochtu-kak-raspoznat-fishingovoe-pismo/, свободный. – Заглавие с экрана. – Яз.рус. (дата обращения: 05.01.2021).

15. Email Security Predictions 2021: 6 Ways Hackers Will Target Businesses. – 2020. – Режим доступа: https://www.vadesecure.com/en/blog/email-security-predictions-6-ways-hackers-will-target-businesses/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 05.01.2021).

16. Group-IB. Прогнозы по киберугрозам, с которыми мир столкнется в новом году. – 2020. – Режим доступа: https://www.group-ib.ru/media/gib-report-2020/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

17. Прогнозы по продвинутым угрозам на 2021 год. – 2020. – Режим доступа: https://securelist.ru/apt-predictions-for-2021/99366/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 07.01.2021).

18. Создание культуры безопасности. – 2019. – Режим доступа: https://www.osp.ru/winitpro /2019/05/13055004/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 05.01.2021).

19. The Hive Docs. – 2020. – Режим доступа: https://github.com/TheHive-Project/TheHiveDocs, свободный. – Заглавие с экрана. – Яз.англ. (дата обращения: 05.01.2021).

20. Примеры фишинговых писем. Типы фишинговых атак и способы их идентификации. – 2019. – Режим доступа: https://bar812.ru/primery-fishingovyh-pisem-tipy-fishingovyh-atak-i-sposoby-ih.html/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 11.01.2021).

References

1. Putyato M. M., Makaryan A. S. Kiberbezopasnost kak neotemlimny atribut mnogourovnevogo zashchishchennogo kiberprostranstva [Cybersecurity as an integral attribute of a multi-layered secure cyberspace]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 3, pp. 94–102.

2. Putyato M. M., Makaryan A. S., Cherkasov A. N., Gorin I. V. Adaptivnaya sistema kompleksnogo obespecheniya bezopasnosti kak element infrastrukturi situacionnogo centra [An adaptive integrated security system as an element of the situation center infrastructure]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 4, pp. 75–84.

3. Ocheredko A. R., Gerasimenko V. S., Putyato M. M., Makaryan A. S. Issledovaniye SIEM-sistem na osnove analiza mekhanizmov vyyavleniya kiberatak [Investigation of SIEM-systems based on the analysis of cyberattack detection mechanisms]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Yestestvenno-*

matematicheskiye i tekhnicheskiye nauki [Bulletin of the Adygea State University. Series 4: Natural-mathematical and technical sciences"], 2020, no. 2, pp. 25–31

4. *Sravnenie system SGRC (Security Governance, Risk, Compliance)* [Comparison of SGRC systems (Security Governance, Risk, Compliance)], 2017. Available at: https://www.anti-malware.ru/compare/russian_sgrc_2017 (accessed 01.04.2021).

5. *Obzor rynka platform reagirovaniya na intsidenty (IRP) v Rossii* [Market overview of incident response platforms (IRP) in Russia], 2018. Available at: https://www.anti-malware.ru/analytics/Market_Analysis/incident-response-platforms-irp-in-russia (accessed 01.11.2021).

6. *Besplatnaya IRP-sistema svoimi silami: opit ispolzovaniya platformi s otkritim kodom The Hive* [Free IRP system in-house: experience of using the open source platform The Hive], 2019. Available at: https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own (accessed 01.12.2021).

7. *Sistema upravleniya intsidentami informatsionnoy bezopasnosti Jet Signal* [Information security incident management system Jet Signal]. Available at: https://jet.su/services/software-development/products/jet-signal/ (accessed 01.12.2021).

8. *Platforma dlya sozdaniya Tsentra reagirovaniya na intsidenty IB* [Platform for creating an Information Security Incident Response Center], Available at: https://rvision.pro/irp/ (accessed 01.12.2021).

9. *Sistemy klassa Incident Response Platform: primeneniye i osnovnyye funktsii* [Incident Response Platform class systems: application and main functions], Available at: https://www.securityvision.ru/products/irp/ (accessed 01.12.2021).

10. *Platforma koordinatsii i avtomatizatsii protsessov reagirovaniya na intsidenty* [Platform for coordination and automation of incident response processes]. Available at: https://www.ibm.com/ru-ru/products/resilient-soar-platform (accessed 01.12.2021).

11. *Security incident response for the masses.* Available at: https://thehive-project.org/ (accessed 01.12.2021).

12. *Sistemy reagirovaniya i upravleniya intsidentami informatsionnoy bezopasnosti (IRP)* [Information Security Incident Response and Management Systems (IRP)], 2019. Available at: https://www.anti-malware.ru/security/irp (accessed 01.12.2021).

13. *The Hive-Project*, 2020. Available at: https://github.com/TheHive-Project/TheHive (accessed 01.05.2021).

14. *Primery fishinga cherez elektronnuyu pochtu: kak raspoznat fishingovoe pismo* [Examples of phishing via email: how to recognize a phishing email], 2020. Available at: http://www.itsec.ru/articles/primery-fishinga-cherez-elektronnuyu-pochtu-kak-raspoznat-fishingovoe-pismo (accessed 01.05.2021).

15. *Email Security Predictions 2021: 6 Ways Hackers Will Target Businesses*, 2020. Available at: https://www.vadesecure.com/en/blog/email-security-predictions-6-ways-hackers-will-target-businesses/ (accessed 01.05.2021).

16. *Group-IB. Prognozi po kiberugrozam, s kotorimi mir stolknetsya v novom godu* [Cyber Threats Predictions the World Will Face in the New Year], 2020. Available at: https://www.group-ib.ru/media/gib-report-2020/ (accessed 01.12.2021).

17. *Prognozy po prodvinutym ugrozam na 2021 god* [Predictions for advanced threats for 2021], 2020. Available at: https://securelist.ru/apt-predictions-for-2021/99366/ (accessed 01.07.2021).

18. *Sozdanie kultury bezopasnosti* [Building a safety culture], 2019. Available at: https://www.osp.ru/winitpro/2019/05/13055004/ (accessed 01.05.2021).

19. *The Hive Docs*, 2020. Available at: https://github.com/TheHive-Project/TheHiveDocs (accessed 01.05.2021).

20. *Primery fishingovikh pisem. Tipi fishingovikh atak i sposoby ikh identifikatsii* [Examples of phishing emails. Types of phishing attacks and how they are identified.], 2019. Available at: https://bar812.ru/primery-fishingovyh-pisem-tipy-fishingovyh-atak-i-sposoby-ih.html/ (accessed 01.11.2021).