УДК 004.056

***С.П. Серёдкин*[1]**

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Россия*

КИБЕРРАЗВЕДКА КАК ЭФФЕКТИВНАЯ СТРАТЕГИЯ ЗАЩИТЫ ОТ УГРОЗ

Аннотация. Настоящая статья посвящена исследованию превентивной защиты корпоративных информационных системс использованием методов кибербразведки. Рассматриваются основные цели, задачи и инструментарий кибербразведки. Учитывая актуальность развития данного направления, автором предложен механизм создания подразделения кибербразведки, а также приведены аргументы необходимости применения данного подхода для обеспечения защиты информации. Современный ландшафт киберугроз постоянно меняется, потенциальными злоумышленниками совершенствуются тактики и техники реализации угроз, в связи с этим вероятность риска нанесения ущерба информационным активам организаций остается достаточно высокой. Все эти факты ведут к поиску новых решений в обеспечении требуемого уровня информационной безопасности, одним из которых и является инструментарий кибербразведки.

Ключевые слова: кибербразведка, киберугрозы, центра мониторинга информационной безопасности.

S.P. Seryodkin1

[1]*Irkutsk State Transport University, Irkutsk, Russia*

Abstract. This article is dedicated to the study of preventive protection of corporate information systems using cyber-intelligence methods. The main objectives of the tasks and tools of cyber intelligence are discussed. Considering the relevance of development of this area, the author proposes a mechanism for creating a cyber-intelligence unit, and also gives arguments for the necessity of applying this approach to ensure information protection. The modern landscape of cyber threats is constantly changing, potential attackers are improving tactics and techniques of threat implementation, therefore the risk of damage to information assets of organizations remains quite high. All these facts lead to the search for new solutions in providing the required level of information security, one of which is the tool of cyber intelligence.

Keywords: cyber intelligence, cyber threats, information security monitoring center.

Введение. Современный рынок информационных технологий стремительно развивается, в связи с этим отрасль информационной безопасности проходит этап жестких испытаний. Высокий уровень подготовленных киберугроз и появление новых уязвимостей в информационных и автоматизированных системах создают высокий уровень рисков как в бизнес-системах, так и в государственных структурах.

Центром противодействия киберугрозам «Innostage CyberART» было проведено исследование киберугроз на российские компании за 2023 год. Поученная статистика по DDoS-атакам и утечкам персональных данных по всей России следующая: 43% утечек произошло у среднего бизнеса, 38% — у малого, 19% — у крупного. Полученные данные подтверждают тот факт, что хакерские группировки объектом кибератак выбирают бизнес [1]. Число кибератак, с которым сталкивается российский бизнес растет с каждым годом. По данным издания «КОМЕРСАНТЪ» статистика неутешительна — в РФ каждая пятая такая атака нацелена именно на средний бизнес, а ущерб от одного подобного инцидента составляет в среднем 5 млн. руб. [2].

Проблематика. Информационная безопасность в настоящее время уже не сводится только к созданию процесса реагирования на уже произошедшие инциденты, современный подход к ИБ включает в себя как реактивные, так и проактивные меры. Именно умение прогнозировать и распознавать атаку по самым ранним признакам становится одним из ключевых факторов защиты бизнеса от киберугроз**.** Одним из инструментов, позволяющим снизить вероятность возникновения инцидентов, а также получить дополнительный контекст для их расследования, является система кибербразведки.

Термин кибербразведка возник путем перевода англоязычного словосочетания Threat Intelligence, который стал популярен примерно 12-15 лет назад.

Основные цели кибербразведки: выявление угроз, защита инфраструктуры, снижение ущерба, поддержка принятия решений.

Задачи, которые необходимо решать: сбор и анализ данных, предоставление разведывательной информации, поддержка операций и прогнозирование.

Парадигма исследования. Современный ландшафт угроз информационной безопасности постоянно изменяется, компании вынуждены быстро адаптироваться и использовать современные инструментарии реагирования на данные обстоятельства с целью недопущения ущерба информационным активам. Актуальность и своевременность использования инструментариев кибербразведки включает в себя добывание необходимой информации об источниках угроз, тактик и техник потенциальных злоумышленников. Полученные данные необходимы для принятия управленческих решений руководством предприятия по реагированию на актуальные угрозы и подготовки оперативных мер защиты.

Процесс обеспечения кибербразведки включает в себя несколько последовательных этапов (рис.1)

1. сбор данных - производится накопление данных, которые формируются в едином формате для последующего хранения и обработки;
2. обработка - предусматривает обработку полученной информации;
3. анализ - анализируются связи и зависимости между отдельными данными, проводится проверка их достоверности и репрезентативности.

Все реализованные мероприятия необходимы для обеспечения дальнейшей работы с полученной информацией.

Взятые таким образом данные необходимо довести до подразделений, чтобы на их основе выстроить защиту информационной системы. В зависимости от типа средств защиты для распространения выбирается формат данных, который ими поддерживается. Необходимо учитывать также методы защиты, которые используются при проведении мониторинга, блокировки и в других защитных мероприятиях.

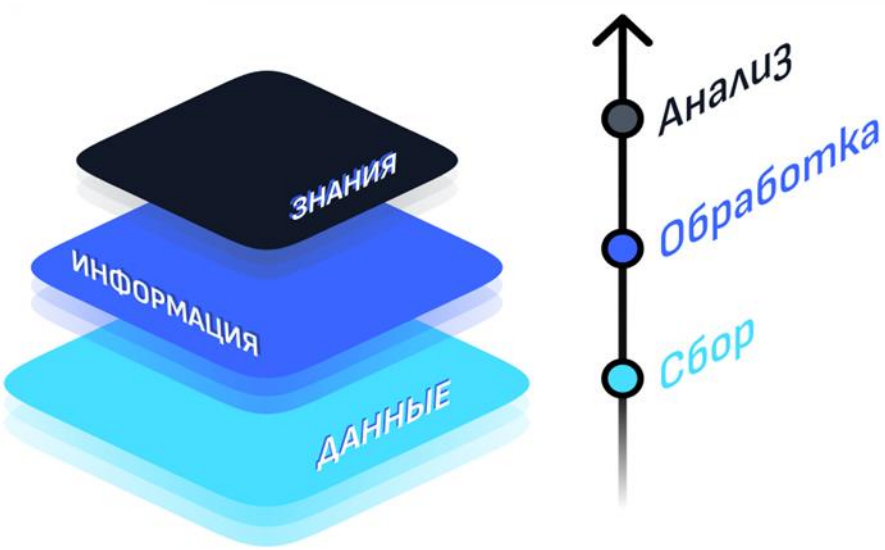

Рис. 1. Процесс кибербразведки

В 2013 году была создана база данных MITRE ATT&CK. Интересен тот факт, что популярнейший в настоящее время инструмент появился благодаря эксперименту, в ходе которого специалисты MITRE попробовали классифицировать действия злоумышленника, чтобы ответить на вопрос «Насколько хорошо мы справляемся с обнаружением задокументированного поведения киберпреступников?». Практически данные действия, в

общем, смогли инициировать инструментарий для служб информационной безопасности по созданию методов кибербразведки. Более детально процесс кибербразведки представлен в документах CREST (Certification center CREST abbreviation - международный центр по аккредитации и сертификации в сфере кибербезопасности) в виде цикличного рис.2. и состоит из следующих этапов:

1 Этап - «Планирование и направление». На этом этапе происходит координация разведывательной деятельности, что позволяет эффективно отвечать на запросы потребителя. Разработка правильного набора требований помогает:

- отслеживать релевантные источники угроз;
- собирать наиболее полезные разведданные;
- готовить аналитические продукты в нужном формате и с нужным уровнем детализации для каждого типа пользователей;
- избегать неэффективной траты времени и средств на сбор и распространение тривиальных данных.

2 Этап - «Сбор данных». На этом этапе собирают данные и информацию в соответствии с требованиями, определенными на предыдущем цикле. Собираемые данные необходимо правильно описать, классифицировать, определить приоритеты реагирования на них.

3 Этап - «Анализ угроз». В ходе анализа необработанные данные и полученная информация сопоставляются, объединяются с другими источниками и превращаются в разведданные. На этом этапе выполняют нормализацию и обработку данных, полученных из всех источников, а затем — непосредственно анализ, для которого необходимо выстроить взаимосвязи, корреляции, влияния разных факторов непосредственно на ту или иную цель. Результатом этого этапа будет получение данных разведки, т.е. тех самых знаний, включая тактики, техники и процедуры действий злоумышленников. Выявление этих тактик и техник позволяет организовать эффективную защиту, создать работающие правила корреляции и при необходимости воссоздать действия злоумышленников для выявления уязвимостей.

4 Этап - «Распространение разведданных и обратная связь». Полученные данные о потенциальных киберугрозах передаются в следующие службы:

- подразделение SOC (Security Operations Center, центр мониторинга и реагирования на инциденты информационной безопасности) — индикаторы компрометации, помощь при расследовании инцидентов, исследования злоумышленников;
- группа по управлению уязвимостями — информация об уязвимостях и эксплойтах к ним;
- группы по предотвращению мошенничества — сообщения об утечке данных сотрудников и клиентов;
- подразделения, обеспечивающие контроль доступа к ресурсам компании — результаты мониторинга даркнета и других источников утечек данных;
- руководители служб безопасности и компании — информация стратегического характера, позволяющая определить тенденции развития киберугроз и соотнести их с рисковой моделью.

Важно на этапе распространения информации об киберугрозах довести данные не только до подразделений, обеспечивающих информационную безопасность, но и до обычных пользователей, тем самым повышая уровень их грамотности и подготовки.

Все представленные этапы реализуются циклично. При этом последний этап хоть и считается заключительным, но не завершает процесс Threat Intelligence, а дает входные данные для первого этапа, который открывает новый цикл. И так может повторяться множество раз, обеспечивая тем самым процесс непрерывности кибербразведки. Именно в обеспечении последовательности и непрерывности процесса кибербразведки достигается цель - предотвращение атаки.

Рис. 2. Цикличность процессов кибербразведки

Практическая реализация. Для создания в предприятии подразделения кибербразведки главным является факт инициирования данного решения со стороны руководства. Понимание руководством важности обеспечения необходимого уровня информационной безопасности, высоких рисков возможных потерь - всё это и является мотиватором в решении данного вопроса. Кадровой основой данного подразделения могут выступать специалисты аналитики по информационной безопасности. При наличии в предприятии SOC (центра мониторинга информационной безопасности) наиболее квалифицированные сотрудники данного подразделения могут составить «ядро» специалистов подразделения кибербразведки. Необходимо чётко регламентировать функции, задачи и механизмы мотивации для сотрудников подразделения, обеспечить всем необходимым для результативной работы.

Для понимания задач, решаемых подразделением кибербразведки, можно рассмотреть обзор платформы кибербразведки Anomali Altitude.

Платформа Anomali не только предоставляет оперативные данные о новых угрозах, но и позволяет проводить комплексный анализ инцидентов, а также автоматизировать исследование индикаторов компрометации.

В состав платформы Anomali Altitude входят решения:

1. Anomali ThreatStream — основной компонент (TIP) — рабочее место аналитика кибербразведки, позволяет собирать, контролировать и анализировать миллионы индикаторов из сотен фидов кибербразведки, работать с операционной и стратегической кибербразведкой, совместно расследовать инциденты безопасности и распространять отчеты, а также экспортировать полученные результаты во внешние системы ИБ, такие как SIEM, NGFW, EDR и другие, для дальнейшего применения. Интерфейс API ThreatStream имеет множество функций, которые позволяют автоматизировано обогащать инциденты при реагировании.

Среди этих функций:

- проверка репутации переданного доменного имени;
- проверка репутации переданного IP;
- получение дополнительных данных для домена или IP для доступных IOC;
- проверка репутации переданного MD5-хэша файла;
- проверка репутации переданного электронного адреса;
- проверка репутации переданного URL;
- отправка файла или URL-адреса в песочницу (вернет ID отчета);

- запрос отчета о файле или URL-адресе, который был отправлен в песочницу (по ID отчета);
- запрос текущего статуса отчета, отправленного в песочницу (по ID отчета);
- добавление тега к указанному IOC для фильтрации связанных сущностей;
- получение отфильтрованных индикаторов по тегу;
- получение списка индикаторов, связанных с переданным именем модели угроз, и ID модели;
- получение HTML-файла с описанием модели угрозы;
- получение списка моделей угроз;
- импорт индикаторов;
- обновление модели угроз безопасности информации по определенным параметрам.

2. Anomali Match — многофункциональная платформа преактивного поиска угроз (хантинга, Threat Hunting- охота на угрозы), сетевой криминалистики и ретроспективного анализа. Данное решение позволяет обнаружить следы компрометации в архиве событий и протоколах трафика глубиной до 10 лет, что значительно превосходит средний период хранения данных в SIEM-системах (1 ─ 6 месяцев).

Уникальность Anomali Match в том, что она позволяет искать сотни миллионов IoC (источником IoC может являться Anomali ThreatStream или другие поставщики подписок STIX\TAXII) в миллиардах событий и потоках трафика в реальном времени, а также в постоянной ретроспективе. Как только Anomali Match получает новые IoC, происходит автоматический ретроспективный анализ. Это достигается с помощью использования технологий Big Data.

Anomali Lens — представляет из себя контент-парсер на базе Natural Language Processing (NLP), распространяемый в виде плагина для браузера (поддерживаются браузеры Firefox, Chrome и Edge (Chromium)). Anomali Lens анализирует и автоматически освещает на веб-страницах и в веб-приложениях те данные, которые могут относиться к угрозам информационной безопасности. В том числе плагин обнаруживает индикаторы компрометации, APT-группировки и их кампании, названия вредоносных файлов, а также техники, тактики и процедуры (TTP) согласно матрице MITRE. Также есть возможность через Lens загружать локальные файлы (PDF, Word, TXT) и сканировать их. По любому выбранному артефакту можно получить общую и контекстную информацию. Также можно моментально проверить есть ли соответствующие угрозы в вашей собственной среде. Кроме того, функционал Lens позволяет экспортировать данные для анализа и проведения расследований в платформе Anomali ThreatStream рис.3.

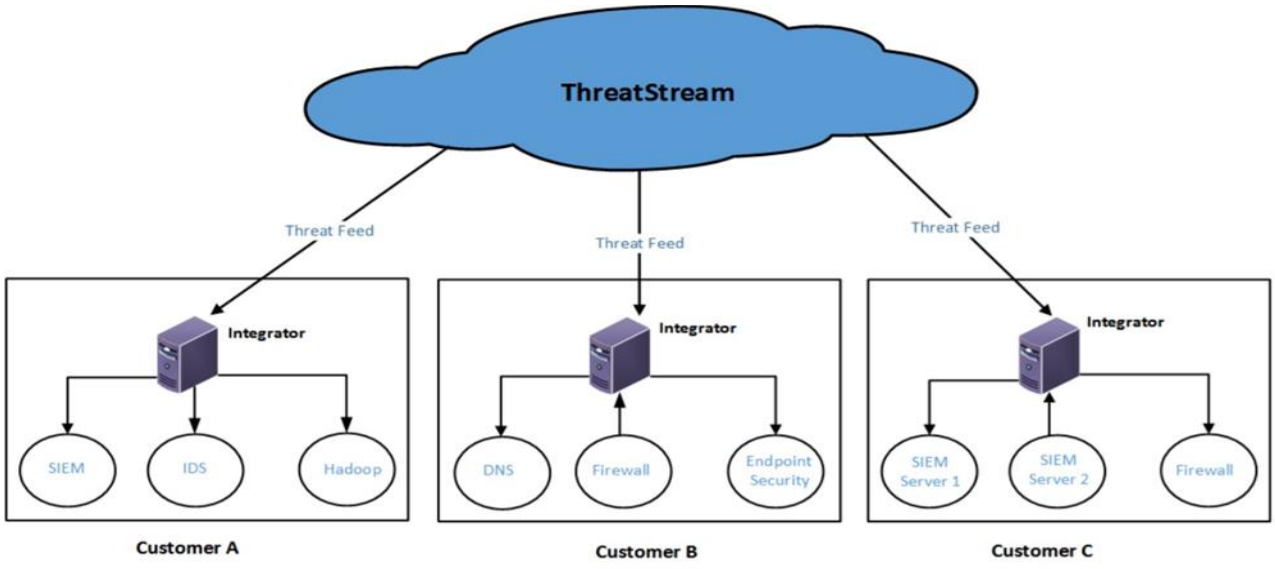

Рис.3. Архитектура с использованием Anomali ThreatStream в облаке

Заключение. Кибербразведка уже стала базовой составляющей стратегии безопасности любой организации, поскольку позволяет своевременно прогнозировать актуальные угрозы и превентивно выстраивать систему защиты от них. Кроме того, кибербразведданные не ограничиваются только индикаторами компрометации, но и дают организациям глубокое понимание того, что происходит за пределами их информационных систем, повышают прозрачность киберугроз, которые представляют наибольший риск для инфраструктуры. Предприятие самостоятельно принимает решение - создавать собственную команду кибербразведки или привлечь внешнего исполнителя, так как это зависит от множества факторов. Главное гарантировать защиту ценных информационных ресурсов для обеспечения штатного режима функционирования бизнес-процессов предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Набиуллин А.А., Захаров С.Д., Юсупов М.Р. Применение технологии threat intelligence в информационной безопасности // Мавлютовские чтения: материалы XV Всероссийской молодежной научной конференции: в 7 томах, Уфа, 26–28 октября 2021 года. – Уфа: Уфимский государственный авиационный технический университет, 2021. – С. 486-494.
2. Гриняев, С.Н., Правдиков Д.И. Основы общей теории киберпространства. Теория боя в киберпространстве // Автономная некоммерческая организация "Центр стратегических оценок и прогнозов", 2018. – 124 с. – ISBN 978-5-906661-21-0.
3. В России набирает популярность кибербразведка. – URL: https://www.tadviser.ru/index.php (дата обращения: 09.12.2024).
4. Каждая пятая атака нацелена на средний бизнес. – URL: https://www.kommersant.ru (дата обращения: 09.12.2024).
5. CREST certificatio. – URL: https://www.crest-approved.org/(дата обращения 09.12.2024).
6. Проактивный анализ киберугроз. – URL: https://www.facct.ru/ 09.12.2024).
7. Искусственный интеллект, импортозамещение, дефицит кадров и другие технотренды 2024 года. – URL: https://rg.ru/2024/01/07/iskusstvennyj-intellekt-importozameshchenie-deficit-kadrov-i-drugie-tehnotrendy-2024-goda.html (дата обращения: 09.12.2024).
8. Что такое центр информационной безопасности (SOC). - URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-a-security-operations-center-soc (дата обращения: 09.12.2024).
9. Автоматизация процессов кибербразведки на основе решений класса Threat Intelligence Platform (TIP).- URL: https://www.anti-malware.ru/practice/methods/threat-intelligence-platform (дата обращения: 09.12.2024).
10. Anomali Threat Stream. - URL: https://www.itsecurityguru.org/2020/03/02/anomali-threat-intelligence-platform/ (дата обращения: 09.12.2024).
11. Сравнительный анализ TIP. - URL: https://vc.ru/u/1036397-vladislav-shabanov/339569-sravnitelnyi-analiz-tip-primenenie-platform-kiberrazvedki-na-primere-anomaly-staxx(дата обращения: 09.12.2024).
12. Обратная связь: как правильно направлять команду к результату. - URL: https://getcompass.ru/blog/posts/obratnaya-svyaz (дата обращения: 09.12.2024).
13. Управление уязвимостями и симуляция атак. -URL: https://softprom.com/ru/ (дата обращения: 09.12.2024).
14. Что такое база MITRE ATT&CK и для чего она нужна? -URL: https://www.securitylab.ru/ (дата обращения: 09.12.2024).

15. Принципы построения центра противодействия киберугрозам. -URL: https://rezbez.ru/article/princzipy-postroeniya-czentra-protivodejstviya-kiberugrozam/ (дата обращения: 09.12.2024).

16. Кибершпионаж. -URL: https://ru.ruwiki.ru/ (дата обращения: 09.12.2024).

17. На что способна кибербразведка. -URL: https://www.securitylab.ru/analytics/479451.php (дата обращения: 09.12.2024).

REFERENCES

1. Nabiullin A.A., Zaharov S.D., Jusupov M.R. Mavljutovskie chtenija: materialy XV Vserossijskoj molodezhnoj nauchnoj konferencii: v 7 tomah. 2021. pp.486-494.

Cyber intelligence is gaining popularity in Russia. – URL: https://www.tadviser.ru/index.php (date of access: 09.12.2024).

2. Grinjaev, S. N., Pravikov D. I. Avtonomnaja nekommercheskaja organizacija "Centr strategicheskih ocenok i prognozov". 2018. P. 124.

4. Every fifth attack is aimed at medium–sized businesses. - URL: https://www.kommersant.ru (date of access: 09.12.2024).

5. CREST certificatio. – URL: https://www.crest-approved.org /(accessed 09.12.2024).

6. Proactive analysis of cyber threats. – URL: https://www.facct.ru / 09.12.2024).

7. Artificial intelligence, import substitution, shortage of personnel and other technological trends in 2024. – URL: https://rg.ru/2024/01/07/iskusstvennyj-intellekt-importozameshchenie-deficit-kadrov-i-drugie-tehnotrendy-2024-goda.html (date of access: 09.12.2024).

8. What is the Information Security Center (SOC). - URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-a-security-operations-center-soc (date of access: 09.12.2024).

9. Automation of cyber intelligence processes based on solutions of the Threat Intelligence Platform (TIP) class. - URL: https://www.anti-malware.ru/practice/methods/th

10. Anomali Threat Stream. - URL: https://www.itsecurityguru.org/2020/03/02/anomali-threat-intelligence-platform / (date of access: 09.12.2024).

11. Comparative analysis of TIP. - URL: https://vc.ru/u/1036397-vladislav-shabanov/339569-sravnitelnyi-analiz-tip-primenenie-platform-kiberrazvedki-na-primere-anomaly-staxx(date of request: 09.12.2024).

12. Feedback: how to properly guide the team to the result. - URL: https://getcompass.ru/blog/posts/obratnaya-svyaz (accessed: 09.12.2024).

13. Vulnerability management and attack simulation. -URL: https://softprom.com/ru / (date of access: 09.12.2024).

14. What is the MITRE ATT&CK database and what is it for? -URL: https://www.securitylab.ru / (date of application: 09.12.2024).

15. Principles of building a center for countering cyber threats. -URL: https://rezbez.ru/article/princzipy-postroeniya-czentra-protivodejstviya-kiberugrozam / (date of access: 09.12.2024).

16. Cyber espionage. -URL: https://ru.ruwiki.ru / (date of application: 09.12.2024).

17. What is it capable of. - URL: https://www.securitylab.ru/analytics/479451.php (date of application: 09.12.2024).

Информация об авторе

Сергей Петрович Серёдкин – к.э.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Author

Sergei Petrovich Seryodkin – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.

Для цитирования

Серёдкин С.П. Кибербразведка как эффективная стратегия защиты от киберугроз// «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2024. – №4. – С. 14-22. – Режим доступа: http://ismm-irgups.ru/toma/424-2024, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 09.12.2024)

For citations

Seredkin S.P. Cyberintelligence as an effective strategy of protection from cyber threats// "Information technologies and mathematical modeling in the management of complex systems": electron. Scientific journal – 2024. – No.4. – P.14-22 – Access mode: http://ismm-irgups.ru/toma/424-2024, free. – Blank from the screen. – Yaz. rus., English (date of reference: 09.12.).