Перспективы развития кибербразведки

В.В. Мухортов, И.Д. Королев, Н.Б. Тимофеев, К.А. Летута

Краснодарское высшее военное училище им. генерала армии С.М.Штеменко

Аннотация: В статье рассматривается развитие кибербразведки, как нового способа обнаружения информационно-технических объектов в киберпространстве, показана ее взаимосвязь с сетевой моделью OSI, определены направления развития систем кибербразведки в повседневных условиях.
Ключевые слова: кибербразведка, классификация, киберпространство, обнаружение, информационно-технические объекты.

Основной особенностью информационно-технических объектов (далее ИТО) является их функционирование кроме общепринятого физического пространства (техносферы), в инфосфере (информационном пространстве; киберпространстве, как глобальном домене внутри инфосферы) [1].

Наблюдается рост их применения в условиях, обладающих сложной радиоэлектронной обстановкой, а также их миниатюризация (робототехнические комплексы, беспилотный автотранспорт, беспилотная авиация и т.д.) и автоматизация, что создает ряд опасностей как с точки зрения безопасности движения, так и с точки зрения общественной безопасности (террористические угрозы, экстремизм, нарушения границ охраняемых объектов и др.) и требует создания эффективных систем обнаружения, способных работать в любых условиях и обстановке, что позволяет применять к ним определенные научно-методические подходы к обнаружению и идентификации [2].

Любой ИТО с точки зрения информационного пространства обладает соответствующим только ему «образом», «слепком», который может включать в себя, например, следующие характеристики: протоколы обмена внутренней информации; IP-адреса; MAC-адреса; протоколы обмена информации с внешней средой; каналы обмена информацией (основные,

запасные); операционные системы; программное обеспечение и другие, которые взаимодействуют с физическим пространством на различных уровнях вне семиуровневой модели OSI: хранилища информации, средства обработки информации, системы приема-передачи информации, устройства энергообеспечения, шины и каналы передачи данных, внешние устройства и системы, системы ретрансляторов и другие элементы, вплоть до космических спутников.

Все ИТО обладают теми или иными системами: системы связи (интегрированные системы связи, оборудование спутниковой связи, беспроводные сети (WLAN, Wi-Fi)); системы оповещения и общие системы сигнализации; системы, используемые для представления обязательной информации для органов государственной власти; системы взаимодействия с внешней средой, информационная система отображения электронных карт, динамическое позиционирование системы, системы, которые взаимодействуют с электронными навигационными системами и системами двигателей, система автоматической идентификации (AIS)); силовое оборудование и системы управления питанием (генератор (двигатель), управление энергопотреблением, интегрированные системы управления, аварийная система, система реагирования на чрезвычайные ситуации); системы сбора данных (радиолокационное оборудование; другие системы мониторинга и сбора данных); системы контроля доступа к ИТО (системы наблюдения, системы сигнализации, системы криптографической защиты информации, системы аутентификации и идентификации); системы управления полезной нагрузкой; системы кибербезопасности (маршрутизаторы, брандмауэры, виртуальные локальные сети, системы обнаружения и предотвращения вторжений, средства антивирусной защиты и т.д.); системы управления (дистанционная автоматическая,

полуавтоматическая); особенности функционирования (индивидуально, в составе группы (роя)) и другие.

В условиях, где физическое пространство изобилует: посторонними излучениями (радиоэлектронным, тепловым, оптико-электронным); акустическими шумами; большим количеством подвижных объектов, обладающих малой эффективной поверхностью рассеивания, эффективность классических способов стремиться к нулю, о чем свидетельствует растущее количество аварийных ситуаций с полуавтономными и автономными системами.

Это позволяет распространить теорию обнаружения объектов в пространстве на новую область существования ИТО – киберпространство, являющегося глобальным доменом внутри информационной сферы, состоящий из взаимосвязанной сети информационно-технологических инфраструктур, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры.

Для изучения объектов в киберпространстве применяются средства кибербразведки.

Кибербразведка – принципиально новый вид технической разведки, появление которой первоначально связано с возникновением концепции информационной войны и переходом основных боевых действий в компьютерное пространство [3-4].

Рассмотрим, что такое кибербразведка, так как в зависимости от контекста, в котором употребляется термин: это может быть, как действие, так и процесс. Различные специалисты имеют разные понятия о кибербразведке. Есть ряд устоявшихся академических терминов, например, от Gartner и SANS Institute [5-7].

SANS Institute, что кибербразведка – набор данных, собранных, оцененных и примененных в отношении угроз безопасности, субъектов

угроз, вредоносных программ, эксплойтов, уязвимостей и индикаторов компрометации.

Компания Gartner считает, что кибербразведка – это знания, основанные на фактических данных о возможных или существующих угрозах, которые включают контекст, индикаторы, последствия, механизмы, практические рекомендации и которые могут быть использованы для принятия решений по реагированию.

В нашем понимании кибербразведка – техническая разведка, осуществляемая путем извлечения и анализа информации, циркулирующей в киберпространстве. Осуществляется путем сбора информации, обрабатываемой в ЭВМ (компьютерах), информационно-телекоммуникационных сетях, ИТО, информации о характеристиках программных, аппаратных и программно-аппаратных средств ЭВМ (компьютеров) и сетей, а также информации об их пользователях, их аватаров и систем искусственного интеллекта.

Рассмотрим классификацию кибербразведки по способу реализации [8]. Можно выделить 9 основных классов кибербразведки по способу реализации: алгоритмическая, аппаратная, вирусная, пользовательская, потоковая, разграничительная, семантическая, сетевая, и форматная.

Алгоритмическая: получение данных путем использования заранее внедренных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей.

Аппаратная: получение информации и данных путем обработки сведений, получения аппаратуры, оборудования и их частей, модулей и их анализа, испытания для выявления их технических характеристик, уязвимостей и не декларированных возможностей, полученных средствами разведки различных видов.

Вирусная: получение данных путем внедрения и применения вирусов (вредоносных программ) в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами.

Вирусная: получение данных путем внедрения и применения вирусов (вредоносных программ) в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами.

Пользовательская: получение информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной легендируемой (заманивающей) информационной инфраструктуре (приманка).

Потоковая: получение информации и данных путем перехвата, обработки и анализа сетевого трафика (систем связи) и выявления структур компьютерных сетей и их технических параметров.

Разграничительная: получение информации из отдельных (локальных) компьютерных систем, возможно и не входящих в состав сети, на основе несанкционированного доступа (НСД) к информации, а также реализация несанкционированного доступа при физическом доступе к похищенным компьютерам или машинным носителям информации (МНИ).

Семантическая: получение индексно-ссылочной и фактографической информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов в целях создания специальных информационных массивов.

Сетевая: получение данных из компьютерных сетей, с помощью зондирования сети, инвентаризации и анализа уязвимостей сетевых ресурсов (и объектов пользователей) и последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскирование своих действий.

Форматная: получение информации и сведений путем «вертикальной» обработки, фильтрации, декодирования и других преобразований форматов представления, передачи и хранения добытых данных в сведения, а затем в информацию для последующего ее представления.

Для наглядности классы кибеpразведки изображены на рис. 1.

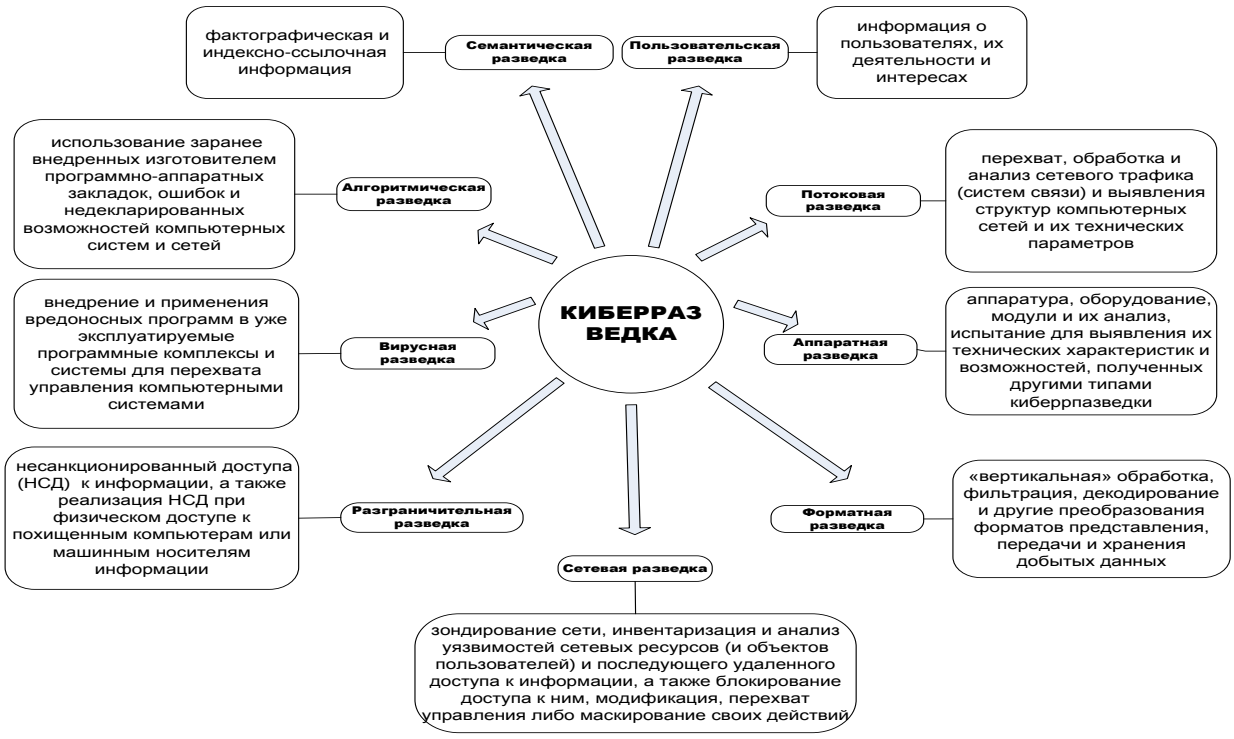

Рис. 1 – Классы кибеpразведки

Кибеpразведка может осуществляться в следующих режимах работы: ручной, полуавтоматический и автоматический.

По наличию оператора систем кибербразведки: автоматическая (без наличия оператора), полуавтоматическая (с частичным привлечением оператора) и ручная (с полным привлечением оператора).

По способу обработки информации: автоматическая (без наличия оператора), полуавтоматическая (с частичным привлечением оператора) и ручная (с полным привлечением оператора).

Как видно из представленных классов, кибербразведкой на бытовом уровне занимается каждый пользователь информационно-технических систем и каждая информационно-техническая (информационная) система в процессе своего функционирования.

Все представленные классы кибербразведки функционируют на своих уровнях согласно типовой модели OSI [9].

Все, что происходит при отправке и приеме данных в локальных сетях и глобальной сети Интернет и, детально описывает модель OSI. Сетевая модель OSI производит операции на семи различных уровнях, иерархически расположенных в следующем порядке: физический уровень, канальный уровень, сетевой уровень, транспортный уровень, сеансовый уровень, уровень представления, прикладной уровень.

На рис. 2 изображены классы кибербразведки с привязкой к модели OSI с учетом модели TCP/IP.

Модель OSI	№	Модель TCP/IP	№	Уровень представления	Классы кибербразведки								
					Семантическая разведка	Алгоритмическая разведка	Вирусная разведка	Разграничительная разведка	Сетевая разведка	Потоковая разведка	Аппаратная разведка	Форматная разведка	Пользовательская разведка
Прикладной уровень	7	Прикладной уровень	4	ПО									
Уровень представления	6			Данные									
Сеансовый уровень	5												
Транспортный уровень	4	Транспортный уровень	3	Сеть									
Сетевой уровень	3	Межсетевой уровень	2	Платформа									
Канальный уровень	2	Уровень доступа к сети	1	Среда									
Физический уровень	1			Платформа									

Рис. 2 – Взаимосвязь классов кибербразведки с моделью OSI

Основной научной проблемой по обнаружению ИТО в физическом пространстве является создание системы координат в киберпространстве с последующей привязкой к физическому пространству.

Координатное пространство должно учитывать все характеристики функционирования ИТО в киберпространстве с учетом модели OSI. Однако согласно рис. 2 с физическим пространством ИТО взаимодействуют на физическом, канальном, сетевом и транспортном уровнях, что позволяет не учитывать ряд будущих осей координат, направленных на описание их положения в киберпространстве.

Для обнаружения ИТО в киберпространстве могут применяться средства кибербразведки работающие с 1-4 уровнями модели OSI и 1-3 уровнями модели TCP/IP, работающими на уровне платформа-сеть, что наглядно представлено на рис. 3.

Модель OSI	№	Модель TCP/IP	№	Уровень представления	Классы кибербразведки								
					Семантическая разведка	Алгоритмическая разведка	Вирусная разведка	Разграничительная разведка	Сетевая разведка	Потоковая разведка	Аппаратная разведка	Форматная разведка	Пользовательская разведка
Прикладной уровень	7	Прикладной уровень	4	ПО									
Уровень представления	6			Данные									
Сеансовый уровень	5												
Транспортный уровень	4	Транспортный уровень	3	Сеть									
Сетевой уровень	3	Межсетевой уровень	2	Платформа									
Канальный уровень	2	Уровень доступа к сети	1	Среда									
Физический уровень	1			Платформа									

Рис. 3 – Применение кибербразведки для обнаружения ИТО в киберпространстве и физическом пространстве

Однако средства кибербразведки, работающие на 5-7 уровне модели OSI и 4 уровне модели TCP/IP могут применяться для идентификации конкретного ИТО, что является одной из важнейших научных и практических задач при создании полностью автономных систем и систем транспортной безопасности [10-12].

Ряд средств кибербразведки находятся в открытом доступе и не имеют существенных ограничений по применению, за исключением средств вирусной разведки, подпадающих под действие Уголовного кодекса Российской Федерации, а также специализированных средств и систем. Например, любая поисковая система «Яндекс», в том числе, встроенная в социальные сети типа «Одноклассники» и «Вконтакте» реализуют алгоритмы, соответствующие целому ряду классов разведки: семантической, алгоритмической, разграничительной, форматной и пользовательской классам кибербразведки [13].

Выводы: развитие систем кибербразведки в условиях глобальной информатизации должно решить ряд научных и практическим проблем, связанных с развитием мобильных полуавтономных и автономных систем, созданием способов и систем противодействия ИТО при организации транспортной безопасности, способов и систем кибербезопасности и охраны объектов, а также способов и систем идентификации ИТО.

Литература

1. Мухортов В.В., Нефедьев Ю.В. Метод оценки живучести информационно-технических объектов по отношению к программно-аппаратным воздействиям // Инженерный вестник Дона. – 2020, №4. URL: ivdon.ru/ru/magazine/archive/N4y2020/6414

2. Фиговский О.Л. В интервале пяти лет появятся инновации, которые сегодня кажутся фантастикой // Инженерный вестник Дона, 2011, №4 URL: ivdon.ru/ru/magazine/archive/n4y2011/643.

3. Антонос, Г.А. Международные измерения права киберпространства the unternational dimuenions of cyberspace law. - Aldershot, 2000. - Vol. 1. - 241 P. (реферат) // Право и информатизация общества: Сб. науч. тр. / Центр социальных науч.-инфор. исслед. Отдел правоведения; РАН. ИГП. Центр

публичного права. Сектор информационного права; Отв. ред. - Бачило И.Л.. – Москва, 2002. – С. 170-182.

4. 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.

5. Королев И.Д., Мухортов В.В. Современные научно-методические подходы к обнаружению и идентификации информационно-технических объектов, перспективы их обнаружения и идентификации в инфосфере // Информационные системы и технологии. – 2022. – № 2(130). – С.100-106. – ISSN 2072-8964.

6. Погружение в Threat Intelligence: кому и зачем нужны данные киберразведки URL: habr.com/ru/company/rvision/blog/552506/ (дата обращения: 01.04.2022).

7. Gylling A., Eliasson P., Ekstedt M., Afzal Z.. Mapping cyber threat intelligence to probabilistic attack graphs // Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, CSR 2021, Virtual, Rhodes, 26–28 июля 2021 года. – Virtual, Rhodes, 2021. – P. 304-311. – DOI 10.1109/CSR51186.2021.9527970.

8. Варламов, О.О. Компьютерная разведка и создание АС до класса защищенности 1Г на основе серттифицированного ПС "ЭЛАР Саперион" // Искусственный интеллект. – 2008. – № 3. – С. 137-144.

9. Авакьянц, А.В., Урубкин М.Ю. Использование моделей TCP/IP и OSI при описании сетевых коммуникаций // Вестник современных исследований. – 2019. – № 1.11(28). – С. 5-10.

10. Минаев В.А., Королев И.Д., Мухортов В.В. Комплексная оценка устойчивости функционирования сложных технических систем в техносфере

и инфосфере. Вопросы радиоэлектроники. 2018;(5):89-94. URL: doi.org/10.21778/2218-5453-2018-5-89-94.

11. Коцарева, И.С., Рябова Е.В., Симонян А.Р. Основные этапы мониторинга по поиску и обнаружению скрытых атак в информационных системах // Международный форум молодых исследователей: Сборник статей Международной научно-практической конференции, Петрозаводск, 09 декабря 2021 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2021. – С. 222-230.

12. 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.

13. Анг Чжо Мьо, Анисимов А.А., Портнов Е.М., Гагарина Л.Г. Методика повышения эффективности управления ресурсоемкими задачами в распределенных вычислительных системах // Инженерный вестник Дона, 2020, №2 URL: ivdon.ru/ru/magazine/archive/N2y2020/6294.

References

1. Muhortov, V.V., Nefed'ev Ju. V. Inzhenernyj vestnik Dona. 2020. № 4. URL: ivdon.ru/ru/magazine/archive/N4y2020/6414

2. Figovskij O.L Inzhenernyj vestnik Dona, 2011, №4 URL: ivdon.ru/ru/magazine/archive/n4y2011/643.

3. Antonos, G. A. Pravo i informatizacija obshhestva. 2002. pp. 170-182.

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

5. Korolev I.D., Mukhortov V.V. Information systems and technologies. 2022. No. 2(130). pp.100-106.

6. Pogruzhenie v Threat Intelligence komu i zachem nuzhny dannye kiberrazvedki [Dive in Threat Intelligence who needs cyber intelligence data and why]. URL: habr.com/ru/company/rvision/blog/552506/ (data obrashhenija: 01.04.2022).

7. Gylling A., Eliasson P., Ekstedt M., Afzal Z. Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience. 2021. pp.304-311. DOI 10.1109/CSR51186.2021.9527970.

8. Varlamov O.O. Iskusstvennyj intellekt. 2008. № 3. P. 137-144.

9. Avak'janc, A.V., Vestnik sovremennyh issledovanij. 2019. № 1.11(28). pp. 5-10.

10. Minaev V.A., Korolev I.D., Muhortov V.V. Voprosy radiojelektroniki. 2018. (5). pp.89-94. URL: doi.org/10.21778/2218-5453-2018-5-89-94.

11. Kocareva I.S., Rjabova E.V., Simonjan A.R. Mezhdunarodnyj forum molodyh issledovatelej: Sbornik statej Mezhdunarodnoj nauchno-prakticheskoj konferencii, Petrozavodsk. 2021. pp.222-230.

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

13. Ang Chzho M'o, Anisimov A.A., Portnov E.M., Gagarina L.G. Inzhenernyj vestnik Dona. 2020. №2. URL: ivdon.ru/ru/magazine/archive/N2y2020/6294.