Применение двух отводящих оптических волокон позволяет реализовать двухканальное преобразование оптических сигналов, что снижает дополнительные погрешности от воздействия внешних влияющих факторов (например, от изгибов оптических волокон, изменения мощности источника излучения при изменении температуры и пр.) [14].

Предлагаемый ВОИП, реализующий новый рефрактометрический способ преобразования сигналов, позволяет повысить чувствительность преобразования оптических сигналов за счет снижения потерь светового потока в микрометрическом оптическом тракте; повысить точность измерения показателя преломления; упростить конструкцию и повысить технологичность оптической системы преобразователя.

Научная значимость работы состоит в:

- повышении достоверности диагностики качества жидкостных сред, как природного, так и техногенного происхождения, за счет использования оптических диагностических признаков – изменения показателя преломления жидкости относительно стандартных образцов конкретного типа жидкости, которые невозможно точно и быстро определить известными средствами измерений;

- определении физико-технических и оптических закономерностей функционирования волоконно-оптических микросистем и базовых ВОИП, основных элементов систем анализа, диагностики и мониторинга качества жидкостных сред.

Исследование выполнено за счет гранта Российского научного фонда № 23-29-10017.

Список литературы

1. Данилов-Данильян В.И. Водные ресурсы мира и перспективы водохозяйственного комплекса России. М.: ООО «Типография ЛЕВКО», Институт устойчивого развития / Центр экологической политики России, 2009. 88 с.

2. Матвеев Ю.И., Малов Н.Д., Корнеев О.Ю., Музалевский А.А., Рыбалко А.Е. Проблема комплексного мониторинга природной среды акваторий и береговой черты Северо-Запада России и формы реализации его результатов в системах принятия решений // Международный экологический конгресс «Новое в экологии и безопасности жизнедеятельности». Доклады. Т. 2. СПб., 14–16 июня 2000 г. С. 112.

3. Зыков В.Н. Метрологические основы систем экологических измерений // Вестник РУДН. Серия: Экология и безопасность жизнедеятельности. 2009. № 1. С. 60-68.

4. Музалевский А.А. Экологическая безопасность и методы ее обеспечения: учебное пособие. СПб.: РГГМУ, 2020. 230 с.

5. Что такое анализ сточных вод для предприятия и какие методы исследований используются? URL: https://o-vode.net/vodosnabzhenie/analiz/stochnyh-dlya-predpriyatiya (дата обращения: 06.02.2024).

6. Балабанов В.И., Журавлева Л.А., Мартынова Н.Б. Инженерная защита окружающей среды: учебник М.: ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, 2022. 233 с.

7. Иванкин А.Н., Олиференко Г.Л., Беляков В.А., Вострикова Н.Л. Физико-химические методы анализа. Спектрометрия: учеб. пособие. М.: МГУЛ, 2016. 127 с.

8. Райхбаум Л.Д. Физические основы спектрального анализа. М.: Наука, 1980.

9. Волкова Г.В. Световодный рефрактометрический датчик контроля химического состава жидких сред: дис. ... канд. техн. наук. Москва, 2004. 145 с.

10. Латышенко К.П. Мониторинг загрязнения окружающей среды: учебник и практикум для среднего профессионального образования. М.: Юрайт, 2019. 375 с.

11. Волков Р.И., Федоров Э.И. Патент на изобретение РФ №2292038. Способ измерения показателя преломления и устройство для его реализации. Опуб. 20.01.2007.

12. Акмаров К.А., Артемьев В.В., Белов Н.П. и др. Промышленные рефлектометры и их применение для контроля химических производств // Приборы. 2012. № 4 (142). С. 1-8.

13. Бадеев В.А., Мурашкина Т.И. Микрорефрактометрический измерительный преобразователь для определения качества жидкостных сред // Труды международного симпозиума «Надежность и качество». 2023. Т. 1. С. 474-476.

14. Бадеева Е.А., Бадеев В.А., Мурашкина Т.И., Серебряков Д.И., Хасаншина Н.А., Васильев Ю.А., Кукушкин А.Н. Патент на изобретение РФ 2796797 С2, Волоконно-оптический способ определения коэффициента преломления прозрачного вещества и реализующий его волоконно-оптический рефрактометрический измерительный преобразователь. Опубл. 29.05.2023.

15. Мурашкина Т.И., Бадеева Е.А. Волоконно-оптические приборы и системы: Научные разработки НТЦ «Нанотехнологии волоконно-оптических систем» Пензенского государственного университета Ч. I / СПб.: Политехника, 2018. 187 с.

ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ КИБЕРИММУНИТЕТА

Кирьянов С.Г.

Российский экономический университет им. Г.В. Плеханова, Москва, e-mail: kslav@list.ru

В истории существует извечное противоборство средств защиты и средств нападения. Кто-то изобретает новую форму наконечника копья, и в противовес этому кто-то придумывает новую многослойную броню. Такой порядок сохранялся на протяжении веков, и сегодняшний день не стал исключением. Сменился лишь вид этого противостояния. Вместо копий – различные вредоносные программы, вместо брони – системы защиты. Сегодня, для обеспечения информационной защиты, уже недостаточно просто настроить антивирус и брандмауэр. Атаки на информацию становятся все более и более продуманными, многоэтапными и полномасштабными. И в противовес этому необходимы новые, свежие подходы к решению вопросов информационной безопасности, как частного лица, так и компаний и, разумеется, государства.

В России, на данный момент, кибериммунный подход разрабатывается и продвигается преимущественно «Лабораторией Касперского». В остальном мире по данному направлению не ведутся активные разработки, по крайней мере в открытом виде.

Лаборатория Касперского начала разработку данной концепции еще в далеком 2002 году. А к 2022 компания уже представила первое устройство, реализующее данный взгляд на построение системы информационной безопасности (ИБ). Представленное устройство представляет из себя защищённый шлюз “Kaspersky IoT Secure Gateway” для обеспечения безопасного соединения интернета вещей с глобальной

или внутренней сетью. Он способен регистрировать события безопасности системы в сети, обнаруживать попытки проникновения во внутреннюю сеть организации и обеспечивать кибербезопасность непосредственно подключенного через этот шлюз устройства.

Таким образом, кибериммунный подход, не смотря на свою новизну, уже не является сугубо теоретической концепцией, а выступает вполне себе реализованным практическим решением, уже доступным на рынке.

Американская исследовательская компания, занимающаяся рынком информационных технологий, сформулировала 10 основных тенденций кибербезопасности в 2023 году [4]:

• Развитие средств управления киберуязвимостью – Поверхность кибератак сегодня достаточно большая и сложная. Необходимо развивать новые меры анализа, прогнозирования и управления киберуязвимостей;

• Создание “иммунитета” среды идентификации и доступа – Системы идентефикации сильно страдают из-за неполноты и различных ошибок конфигурации. Системы идентификации не защищаю все компоненты;

• Консолидация платформ кибербезопасности – Информационные системы безопасности упрощаются и стремятся обеспечить исполнение одной основной задачи. Важно пересматривать имеющиеся средства безопасности и устранять избыточность;

• Компонуемая безопасность – Необходимо перейти от использования монолитного приложения безопасности к построению модульных систем, в которых каждый компонент возможно заменять.

Среди этих 10 тенденций кибериммунитет отвечает четырем из них, что безусловно говорит о его актуальности для текущего времени.

Кибериммунитет – аналог иммунитета в живой природе

Люди очень часто заимствуют из природы различные идеи, концепты и подходы, ведь это очень надежный и важный источник отлично проработанных механизмов. Растительный, животный и даже микроскопический мир подарили человечеству множество идей, таких как: гидролокация, инфракрасное зрение, закрылки и многое другое. Позаимствовали люди и более абстрактные вещи, идеи и даже названия, вроде муравьиного алгоритма или схемы в виде деревьев.

Разумеется, не обошёл такой подход компьютерные системы и информационную безопасность в частности. Такие понятия как вирусы и сетевые черви давно перестали ассоциироваться с сугубо биологическим понятием. И подход к построению системы защиты организации, рассматриваемый в данной работе, также построен на известной системе жизнеобеспечения человека – на иммунной системе.

У каждого живого существа есть этот важнейший механизм. Она представляет из себя сложнейшую систему, состоящую из тесного взаимодействия множества различных структур организма. Эта система, с помощью множества различных химических реакций, неустанно бдит за устойчивостью функционирования своего организма и оперативно принимает меры по устранению различных вмешательств извне.

Иммунная система способна идентифицировать множество различных вредных патогенов и для каждого из них подготовить свой ответ. При этом она успешно отделяет клетки собственного организма от зараженных, не нарушая работу всего организма.

У иммунной системы есть несколько слоев защиты: механический, химический и биологический. Кожа, панцири, скорлупа и прочие подобные барьеры обеспечивают первичную, механическую защиту, от попадания чего-либо из враждебной окружающей среды во внутрь организма. Химическая защита представлена эпителием, который путем выделения различных химических соединений обеззараживает то, что должно попасть в организм. Легкие, желудочно-кишечный тракт и мочеполовая системы как раз используют подобный химический барьер. Биологический слой защиты представляет из себя симбиоз с огромным множеством микроорганизмов, которые создают собственную микрофлору внутри организма носителя и дают явный отпор различным патогенным микроорганизмам, попавшим в их поле зрения.

Существуют различные виды иммунитета: врожденный, полученный по наследству и адаптивный, сформированный в течении жизни после перенесенных заболеваний или с помощью вакцин (рис. 1).

Таким образом, в технике и, в частности, в области информационных систем по аналогии с живой природой также могут быть реализованы подобные механизмы, обеспечивающие защиту от различных вредоносных воздействий как извне, так и внутри.

Особенности кибериммунитета

Кибериммунитет – это прежде всего комплексный подход к организации защиты IT-систем. Подобно биологическому иммунитету, кибериммунитет имеет собственные механизмы обнаружения угроз: различные платформы реагирования на инциденты (IRP), системы управления информацией о безопасности (SIEM), а также слои защиты, изолирующие систему от внешней среды – Firewall, интернет фильтры и д.р. Главное в кибериммунном подходе то, что средства и механизмы защиты используются одновременно, дополняя друг друга в единой системе безопасности.

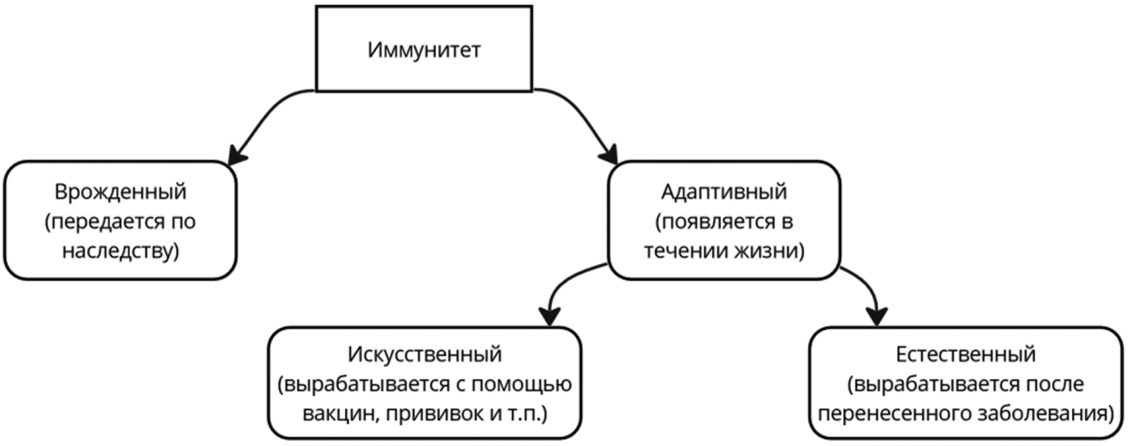

Рис. 1. Виды иммунитета в живой природе

Отсюда и идет биологическое сравнение, так как данная система информационной безопасности очень сильно напоминает биологический иммунитет.

Можно выделить следующие принципы, характерные для построения кибериммунной системы [1-2]:

1. Следование принципу «secure by design»;
2. Создание и развертывание системы обнаружения инцидентов безопасности;
3. Использование систем контроля активности;
4. Организация доменов безопасности путем отделения компонентов системы друг от друга с помощью различных барьеров защиты;
5. Использование нескольких независимых друг от друга уровней защиты;
6. Создание и использование систем, обеспечивающих контрмеры против различных инцидентов безопасности.

Принцип «secure by design» заключается в том, что для упрощения построения системы защиты и значительного повышения ее эффективности необходимо начинать разрабатывать систему безопасности еще на этапе проектирования основной системы. Так как порой небольшое изменение архитектуры системы способствует многократно более серьезному изменению в безопасности этой самой системы.

Подобно биологическому иммунитету, его кибер версия должна успешно находить и определять различные инциденты безопасности, вроде несанкционированного проникновения, различных подозрительных действий в системе или обнаружение следов работы вредоносного ПО. По своей сути подобные механизмы уже давно используются на рынке кибербезопасности, например, различные платформы реагирования на инциденты (IRP), системы управления информацией о безопасности (SIEM) и другие.

Использование систем контроля активности подразумевает, что все происходящие процессы в системе не должны быть скрыты от системы кибериммунитета. В частности, иммунитет человека использует принцип белого списка, т.е. допускает наличие только строго определенных элементов. Все остальные же отмечаются им как вредоносные и выводятся из организма. Кибериммунитет должен действовать аналогичным образом.

В любой системе с помощью специального программного обеспечения по мониторингу активности, вроде “ИНСАЙДЕР” или “StaffCop”, можно собрать статистику рабочей деятельности: какие ресурсы задействуются, какие действия совершаются, что пересылается и прочее. А если дополнить статистику данными, собранными из систем предотвращения утечек (DLP) и/или систем управления информацией о безопасности (SIEM), у владельца системы сформируется полная картина операционной деятельности этой самой системы. А также на основе этой статистики возможно составление белого список разрешенных действий, которые кибериммунитет будет считать за допустимые для исполнения, тем самым существенно ограничивая деятельность злоумышленников.

Отделение компонентов системы друг от друга с помощью различных барьеров защиты – невероятно важный подход к защите систем. Зачастую, системы безопасности настроены на предотвращение атак извне системы. Злоумышленнику бывает достаточно проникнуть сквозь внешний барьер, например, авторизоваться как пользователь системы, и информационная защита начинает трещать по швам.

Подобное разделение Касперский предлагает провести и для программного обеспечения. Более того, вместе с разделением возможно использовать и минимизацию доверенной вычислительной базы (ДВБ) [1].

Рис. 2. Пример разделения компонентов системы в KasperskyOS на домены безопасности [1]

Это подразумевает использование как можно меньшего количества кода в ядре программы или операционной системы, который будет осуществлять только самые основные, критичные для работы системы механизмы. Все остальное же предлагается вынести в отдельные компоненты [1].

Биологический иммунитет работает не только на границе организма и внешнего мира, но и внутри организма тоже. Каждый орган человека защищен по-своему и имеет некоторую собственную систему защиты. Если вредоносный патоген прошел через внешний рубеж организма, то у внутреннего рубежа еще есть возможность его остановить.

И, соответственно, кибериммунитет должен работать по этой же аналогии. Нельзя полагаться на то, что внутренняя сеть безопасна или соседний компонент системы можно считать “доверительным”. Должна быть собственная защита у каждого компонента системы.

Как иммунная система имеет несколько слоев защиты: механический, химический и биологический, так и кибериммунная система также должна иметь несколько слоев защиты. Это могут быть и физические ограничения, вроде использования только проводных каналов связи, использование сетевых шлюзов или физического ограничения доступа к компонентам системы. Можно использовать различные программно-аппаратные средства, вроде фаерволов, IDS или аппаратных шифраторов, в том числе математические и организационные методы защиты. Защищаемые компоненты информационной системы группируются в домены безопасности, в рамках каждого из которых реализуется политика безопасности с определенными требованиями.

Подобная доменная структура может быть сформирована по-разному, в соответствии с различными требования системы и организации. Общий, типовой случай разделения на домены безопасности приведен на рисунке 3.

В конечном итоге, группировать эти защитные средства можно по разным категориям, но главное – это их совместное использование. Нельзя ограничиваться только одной категорией защиты.

И последний компонент кибериммунной системы – это система контрмер. Природный иммунитет не ограничивается только детектированием вредоносного вторжения, он организует специально подобранную ответную реакцию на внешний патоген. Следовательно, и кибериммунитет должен отвечать на инциденты безопасности оперативно и адекватно. Просто обнаружить подозрительную активность и внести ее в лог недостаточно в современных реалиях. Необходим быстрый и автоматический ответ, который окажет минимальное воздействие на штатную деятельность системы, но при этом позволит защититься от вредоносного воздействия

Рис. 3. типовое разделение на домены безопасности в сети организации [5]

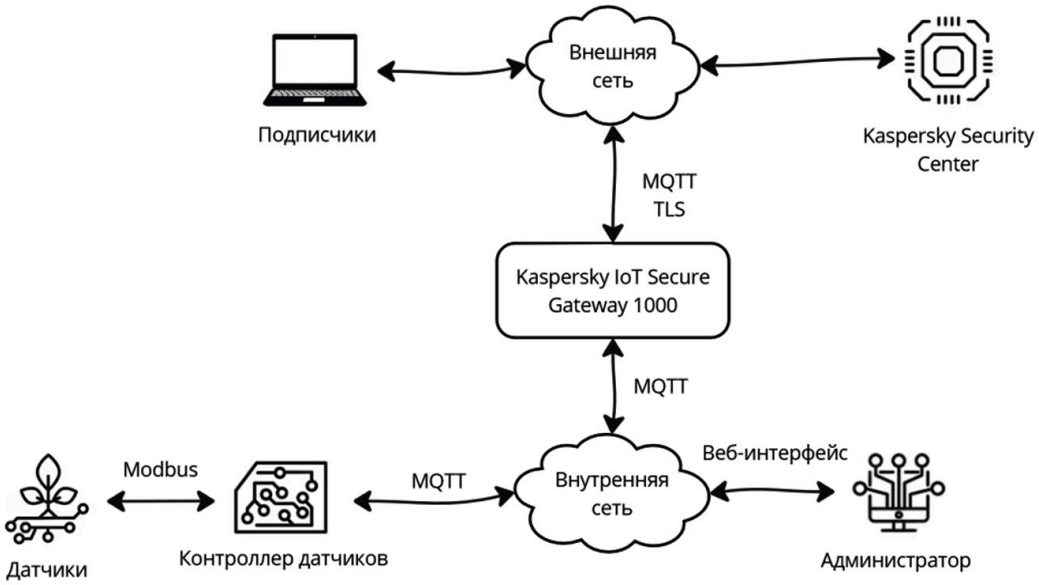

Рис. 4. Типовая схема использования Kaspersky IoT Secure Gateway 1000

Кибериммунный подход запатентовала Лаборатория Касперского в 2022 году [3]. На сегодняшний день эта компания является пионером в данном направлении. Лаборатория Касперского уже представила первый аппаратные решения, позволяющие реализовать кибериммунную систему на практике.

Kaspersky IoT Secure Gateway 1000 – это кибериммунная информационная система на базе их собственной операционной системы

KasperskyOS. Основной её задачей является быть безопасным шлюзом для интернета вещей.

Как пример ранней кибериммунной системы, на рисунке 4 приведена схема типового использования подобного устройства в сети фирмы. Протоколы обмена данных на схеме приведены лишь примерно, для наглядности, а в реальной ситуации пользователь в праве использовать любой удобный протокол передачи данных.

Рисунок отражает реализацию кибериммунной системы при использовании технологии интернета вещей (IoT). Данные с датчиков, фиксирующих параметры функционирования производственного оборудования, а также аномальные события, связанные с действиями нарушителей, передаются в шлюз, реализующий функции кибериммунной системы. Датчики используют протокол передачи данных Modbus, через контроллер датчиков передают данные о функционировании системы во внутреннюю сеть фирмы. Также данные необходимо передать некоторым внешним подписчикам. Ими могут быть сервера обработки данных, удаленные администраторы и т.д. Решение Kaspersky IoT Secure Gateway 1000 выполняет функцию защитного шлюза, между внутренней и внешней сетью обеспечивая безопасность передачи данных и защищенность каналов передачи.

Заключение

Проведенный анализ кибериммунного подхода показывает, что это перспективное и актуальное направление развития систем информационной безопасности. Активные и стремительные разработки Лаборатории Касперского лишь подтверждают эти выводы.

Система кибериммунитета – это прежде всего комплексный подход к совершенствованию системы информационной безопасности. Кибериммунная система закладывается еще на стадии проектирования архитектуры всей системы, и благодаря этому проектирование подсистемы защиты не происходит в отрыве от разработки самой системы.

Помимо глубокого интегрирования с целевой системой, кибериммунитет подразумевает использование множества разных механизмов защиты в единой системе безопасности. Благодаря такому комплексному подходу, данный метод позволит успешно противостоять как известным угрозам, так и угрозам нулевого дня, что, безусловно, является одним из важнейших вызовов в целом для сферы информационной безопасности.

Построение кибериммунных систем задает тенденцию к уходу от монолитных, неповоротливых систем защиты к более модульным и вариативным, что позволит снизить стоимость внедрения защиты.

В перспективе данный подход способен привести к полному пересмотру принципов построения архитектуры безопасности, а также стимулировать разработку модульных аппаратно-программных средств информационной защиты. Появление подобных модульных систем защиты может существенно упростить задачу управления инцидентами безопасности, так как большинство подобных задач в будущем может решаться в автоматическом режиме, без тонкой настройки и привлечение узких специалистов.

Возможно, как и во многих других случаях, подобная интерпретация биологического механизма поможет существенно улучшить сферу обеспечения информационной безопасности.

Список литературы

1. Технологии и методологии. Кибериммунитет. [Электронный ресурс]. URL: https://os.kaspersky.ru/technologies/cyber-immunity/ (дата обращения: 20.10.2023).

2. Биологическая метафора кибер-иммунитета. [Электронный ресурс]. URL: https://scm.etu.ru/assets/files/2023/sbornik/217-220.pdf (дата обращения: 22.10.2023).

3. «Лаборатория Касперского» обозначила притязания. [Электронный ресурс]. URL: https://www.comnews.ru/content/223684/2022-12-26/2022-w52/laboratoriya-kaspers kogo-oboznachila-prityazaniya (дата обращения: 26.10.2023).

4. Gartner Identifies the Top Cybersecurity Trends for 2023. [Электронный ресурс]. URL: https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023 (дата обращения: 27.10.2023).

5. Dallas Lock: контроль безопасности ИТ-инфраструктуры предприятия. [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Enterprise-IT-security-with-Dallas-Lock (дата обращения: 27.10.2023).

К ВОПРОСУ О НЕОБХОДИМОСТИ УПРАВЛЕНИЯ РИСКАМИ В ПОВЕРОЧНОЙ ДЕЯТЕЛЬНОСТИ МЕТРОЛОГИЧЕСКОЙ СЛУЖБЫ ООО «АСУ ПРО»

Лабутина С.А.

ФГБОУ ВО «Оренбургский государственный университет», Оренбург, e-mail: labutina_sa@mail.ru

ООО «АСУ ПРО» – аккредитованная в области поверки средств измерений (СИ) организация, она имеет свидетельство о регистрации в Российской системе калибровки, а также аттестат аккредитации, удостоверяющий легитимность проведения метрологической экспертизы. Метрологическая экспертиза проводится метрологической службой (МС), представляющей структурное подразделение организации (рис. 1). Документация системы менеджмента качества (рис. 2) – это внутренние документы, регламентирующие порядок осуществления деятельности (процессов системы менеджмента качества), обеспечивающие выполнение функций управления путем определения форм и видов взаимодействия всех подразделений предприятия.