УДК 004.056.53

***С.П. Серёдкин*[1]**

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

ОСОБЕННОСТИ КИБЕРАТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В СОВРЕМЕННЫХ УСЛОВИЯХ

Аннотация. Беспрецедентное количество кибератак на информационную инфраструктуру в том числе на объекты критической информационной инфраструктуры (КИИ) в 2022 году, требует от государственных учреждений и бизнеса четкой скоординированной позиции по вопросам противодействия кибератакам и обеспечения устойчивого функционирования всех сфер экономики. Настоящая статья посвящена исследованию современных причин возникновения вредоносной киберактивности в отношении сфер экономики России, истории и эволюции кибератак в мире. Приведена хронология крупнейших кибератак и их последствий. Дан анализ современным кибератакам на критические инфраструктуры как форме агрессии. Представлено современное состояние кибербезопасности объектов КИИ, а также основные источники и способы реализации атак на информационные ресурсы. Приведена статистика киберугроз на информационные ресурсы РФ и последствия от кибератак по сферам деятельности.

Показан текущий обзор мер законодательного и организационного характера по выработке незамедлительных мер по противодействию кибератакам в отношении объектов КИИ. Проанализированы решения отечественных производителей средств защиты информации по построению комплексной защиты объектов.

Подчеркнута важная роль в построении системы противодействия кибератакам основанная на взаимодействии субъектов КИИ с регуляторами в сфере обеспечения защиты информации РФ для обеспечения безопасности объектов КИИ как основного приоритетного направления обеспечения национальной безопасности.

Ключевые слова: Кибератака, хакинг, Критическая информационная инфраструктура (КИИ), Федеральная служба по техническому и экспортному контролю (ФСТЭК), Государственная система обнаружения, предупреждения кибератак (ГосСОПКА), Национальный координационный центр по компьютерным инцидентам (НКЦКИ), информационная безопасность (ИБ).

***S.P. Seryodkin*[1]**

[1]*Irkutsk State Transport University, Irkutsk, Russian Federation*

REVIEW OF REGULATORY AND LEGAL ACTS TO ENSURE THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

Abstract. The unprecedented number of cyberattacks on the information infrastructure, including critical information infrastructure (CII) facilities in 2022, requires government agencies and businesses to have a clear coordinated position on countering cyberattacks and ensuring the sustainable functioning of all sectors of the economy. This article is devoted to the study of the modern causes of malicious cyber activity in relation to the spheres of the Russian economy, the history and evolution of cyber-attacks in the world. The chronology of the largest cyberattacks and their consequences is given. The analysis of modern cyberattacks on critical infrastructures as a form of aggression is given. The article presents the current state of cybersecurity of CII facilities, as well as the main sources and methods of implementing attacks on information resources. The statistics of cyber threats to the information resources of the Russian Federation and the consequences of cyber-attacks by spheres of activity are given. The current review of legislative and organizational measures to develop immediate counteraction measures is shown.

Keywords: Cyberattack, hacking, Critical Information Infrastructure (CII), Federal Service for Technical and Export Control (FSTEC), State System for Detecting and Preventing Cyberattacks (GosSOPKA), National Coordination Center for Computer Incidents (NCCI), Information Security (IS).

Введение. Протекающий в настоящее время процесс формирования нового миропорядка сопровождается нарастанием уровня трансграничных угроз безопасности суверенных государств и всего мирового сообщества. Эти угрозы и вызовы приобрели настолько сильный и системный характер, что создают реальную опасность для современной цивилизации. К числу таких угроз относятся: распространение оружия массового уничтожения, международный терроризм, наркоторговля, организованная преступность, дефицит ресурсов и продовольствия, незаконная миграция, изменение климата и многое другое. Наиболее стремительными темпами в последние десятилетия нарастают угрозы,

связанные с информационной безопасностью, – важнейшим элементом безопасности современных государств и неотъемлемым фактором формирования системы международных отношений[1].Современный уровень развития информационных технологий способствует стиранию границ между государствами в коммуникационном пространстве, созданию беспрецедентных возможностей для воздействия на огромные массы населения с применением разного рода информационных средств и методов.

Формирование нового миропорядка происходит в условиях нарастающей глобальной нестабильности и хаотизации международных отношений, в которых устойчивость политических режимов государств зависит от их способности противостоять «цветным революциям», гибридным войнам, кибератакам и технологиям управляемого хаоса [2]. Современная ситуация в мире доказывает, что идет переход к многополярному миру, это происходит на фоне продолжающегося формирования глобального информационного пространства. Мировое сообщество все более активно использует информацию как орудие в достижении превосходства в различных сферах жизни общества – социальной, духовной, экономической. Но прежде всего – в политической.

В настоящее время наша страна подвергается беспрецедентному информационному воздействию, которое по своей агрессивности превосходят накал самых мрачных периодов «холодной войны».

Отечественные спецслужбы характеризуют уровень кибератак на РФ, как «критический». Главным вызовом 2022 г. для сферы информационной безопасности в России стал беспрецедентный рост вредоносной киберактивности. Как факт эта тенденция была отмечена в рамках заседания Совета Безопасности 20 мая 2022г [3].Эксперты «Лаборатории Касперского» опубликовали исследование, в котором сообщили о росте количества целевых кибератак на промышленные предприятия в России. Чаще всего вредоносные объекты проникают на компьютеры автоматизированных систем управления из интернета, кроме того стало известно об измененной тактике хакерских атак в России. Киберпреступники сосредоточилась на нападении на серверы баз данных - их доля в общем числе утечки составила 68%. Кроме того, к кибератакам на объекты КИИ подключились различные группы хактивистов, начав активно атаковать компании, относящиеся к важным секторам экономики с позиции обеспечения национальной безопасности. Согласно источника[4] хакеры получают доступ к серверам с помощью заражения рабочих мест ИТ-специалистов вредоносным ПО, которое помогает красть пароли и сессионные файлы cookie, с помощью поиска и эксплуатации уязвимостей в системах удаленного доступа, а также в самих CMS (системах управления контентом). Российские разработчики решений для детектирования и предотвращения кибератак, подтверждают тенденцию увеличения в 2022 году количества незащищенных баз в России, количество которых выросло на 37% Причиной стало недостаточное внимание разработчиков, администраторов и архитекторов баз к безопасности, наличие уязвимостей в используемых продуктах и решениях, а также неправильная конфигурация.

Понимая сложность ситуации, которая вызвана ростом числа атак на критическую информационную инфраструктуру Российской Федерации и необходимостью принятия всеобъемлющих мер по противодействию кибератакам, тема обеспечения информационной безопасности является одной из наиболее актуальных. Исследованию вопросов по анализу кибератак на объекты КИИ способам и мерам противодействия посвящена настоящая работа.

История эволюции кибератак. В первые теория, лежащая в основе компьютерных вирусов, была опубликована в 1949 году Джоном фон Нейманом, пионером компьютерных технологий, который высказал факт, что компьютерные программы могут самовоспроизводиться [5]. В конце 1950-х возник так называемый «телефонный фрикинг». «Фрикерами» называли людей с особым интересом к принципу работы телефонов. Фрикинг охватывает несколько методов перехвата протоколов, использовавшихся инженерами телекоммуникационных сетей для удаленной работы, что позволяло телефонным

мошенникам совершать бесплатные звонки на дальние расстояния, уклоняясь от их оплаты. В середине 1960-х большинство компьютеров было огромными мэйнфреймами, закрытыми в защищенных помещениях с контролируемой температурой. Эти машины были очень дороги, поэтому доступ (даже для программистов) оставался ограниченным. В 1967 компания IBM пригласила школьников опробовать свой новый компьютер. После изучения доступной части системы ученики начали копать глубже, изучая ее язык и получая доступ к другим ее частям. Это был ценный урок для компании, выразившей признательность «нескольким старшеклассникам за их непреодолимое желание взорвать систему». Это повлекло разработку защитных мер и, возможно, заложило основы нацеленности на безопасность, которая с тех пор будет необходима разработчикам. Этичный взлом, или хакинг, практикуется по сей день. История кибербезопасности начинается в 1972 году с исследовательского проекта ARPANET (сеть агентства перспективных исследовательских проектов) — предшественника Интернета. Исследователь Боб Томас создал компьютерную программу под названием Creeper, которая могла перемещаться по сети ARPANET, оставляя за собой навигационную цепочку. Она оставляла запись: «I'm the creeper, catch me if you can». Рэй Томлинсон, изобретатель электронной почты, написал программу Reaper, которая преследовала и удаляла Creeper. Программа Reaper была не только первым примером антивирусного программного обеспечения, но и первой самовоспроизводящейся программой, что сделало ее первым компьютерным червем. В 1972–1974 годах в научных трудах возникают дискуссии о компьютерной безопасности. Государственные ведомства ESD и ARPA вместе с ВВС США и другими организациями, которые работали над совместной разработкой проекта ядра безопасности для компьютерной системы Honeywell Multics (HIS level 68), создали одну из первых систем компьютерной безопасности. Калифорнийский университет в Лос-Анджелесе и Стэнфордский исследовательский институт работали над аналогичными проектами [6].В 1979 году 16-летний Кевин Митник взломал The Ark (компьютер Digital Equipment Corporation, используемый для разработки операционных систем) и сделал копии программного обеспечения. В 1980-е увеличилось количество громких атак, в том числе — на National CSS, AT&T и Los Alamos National Laboratory. В 1983 году впервые были использованы термины «троянский конь» и «компьютерный вирус». В 1985 году Министерство обороны США опубликовало «Критерии определения безопасности компьютерных систем» (также известные как «Оранжевая книга»), в которых содержалось руководство по следующим вопросам:1. оценка степени доверия программному обеспечению, обрабатывающему секретную или другую конфиденциальную информацию;2. меры безопасности, которые производителям нужно было встраивать в свои коммерческие продукты. В 1987 году появился первый коммерческий антивирус, хотя по поводу личности изобретателя первого антивирусного продукта ведутся споры. В 1990 году были созданы первые полиморфные вирусы (код, который мутирует, сохраняя при этом исходный алгоритм, чтобы избежать обнаружения), в этом же году был основан EICAR — Европейский институт компьютерных антивирусных исследований. Количество новых вирусов и вредоносных программ резко возросло в 1990-х: с десятков тысяч в начале десятилетия до 5 миллионов ежегодно к 2007. К середине 90-х стало ясно, что кибербезопасность должна быть массовой [5]. По данным ресурса [6] общее кумулятивное количество образцов вредоносного ПО в 2022 году составит 1 347,39 миллиона.

Современная кибератака на критическую инфраструктуру как форма агрессии. Кибератака является современной формой агрессии, совершаемой отдельными лицами, либо целой группой лиц, целью которой является подрыв информационной системы безопасности, подрыв работы какой-либо инфраструктуры, компьютерной сети и/или подрыв работы персональных компьютеров и других приспособлений, произведенный любыми способами [7].

Крупнейшие кибератаки на КИИ:

- 2010-2012 гг. Атака Stuxnet на Иран. Это первый известный компьютерный червь, перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами марки Simatic S7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens;
- Апрель 2016 г. Шифровальщик Petya. Стандартный сценарий заражения выглядит следующим образом: HR-специалист получает письмо со ссылкой на Dropbox, по которой можно перейти и скачать «резюме». Файл по ссылке является самораспаковывающимся архивом с расширением .EXE. Программа шифрует файлы на жёстком диске компьютера-жертвы, а также перезаписывает и шифрует MBR — данные, необходимые для загрузки операционной системы. В результате все хранящиеся на компьютере файлы становятся недоступными. Затем программа требует денежный выкуп в биткойнах за расшифровку и восстановление доступа к файлам;
- Май 2017 г. Шифровальщик WannaCry. Заразил более 500 тысяч устройств по всему миру и причинил ущерб на 4 млрд долл. К шифровальщику был добавлен эксплойт EternalBlue, использовавший уязвимости Windows. С помощью EternalBlue троян проникал в сеть и устанавливал WannaCry на компьютер жертвы. Затем WannaCry продолжал распространяться по другим устройствам в локальной сети. В зараженной системе WannaCry шифровал файлы и требовал выкуп;
- Июль 2017 г. Вайпер NotPetya (ExPetr). Проникал в сеть через обновление украинского ПО для подачи финансовой отчетности в контролирующие органы (злоумышленникам удалось скомпрометировать инфраструктуру компании-разработчика) и распространялся по компьютерам подобно WannaCry. NotPetya шифровал файловую таблицу таким образом, что ее дешифровка была невозможна даже после выкупа. Общий ущерб превысил 10 млрд долл. (около 730 млрд руб.);
- Февраль 2017 г. Шифровальщик Erebus. Был замечен в распространении с помощью зараженного дистрибутива VLC медиа-плеера. Также может распространяться с помощью email-спама и вредоносных вложений, эксплойтов, фальшивых обновлений, перепакованных и заражённых инсталляторов. Южнокорейская веб-хостинговая компания Nayana согласилась выплатить 1 млн долл. за разблокировку компьютеров, пораженных шифровальщиком Erebus;
- Январь 2018 г. Шифровальщик SamSam. Вирус заблокировал файловую систему клиники Hancock Health в США, требуя выкуп за дешифровку. Все файлы в сетях больницы были зашифрованы. ИТ-сотрудники больницы распорядились выключить все компьютеры медучреждения, чтобы не допустить дальнейшего распространения инфекции по сети;
- Март 2019 г. Атака на Norsk Hydro. В результате атаки шифровальщика пострадали как офисные, так и технологические процессы;
- Июнь 2019 г. Атака на ASCO. ASCO, один из крупнейших в мире поставщиков запчастей для авиационной техники, прекратил производство на заводах в четырех странах из-за вируса-вымогателя, появившегося на производственной площадке в Завентеме, Бельгия. Неясно, согласилась ли ASCO выплатить выкуп за восстановление доступа к своим системам, восстановила их из резервных копий или приобрела новые системы и восстановила компьютерную сеть с нуля;
- Декабрь 2019 г. Атака на сеть дата-центров в США. Компания CyrusOne была атакована версией вируса-вымогателя REvil (Sodinokibi). К началу декабря 2019 года у CyrusOne насчитывается 45 дата-центров в Европе, Азии, Южной и Северной Америке. Услугами компании пользуются более тысячи клиентов. Выкуп заплачен не был, работоспособность сети восстановлена самостоятельно;
- Декабрь 2019 г. Атака на госорганы в Луизиане. Всплеск атак, которые включали в себя фишинг и вымогательства. В 11 часов злоумышленники нанесли окончательный удар и

американские города оказались под атакой вируса-вымогателя, который заражает компьютерную технику местных служб программой для шифровки данных;

- Январь 2020 г. Шифровальщик Snake. Snake шифрует самые разные файлы, однако специально обходит системные папки. Первыми жертвами Snake стали автомобильный производитель Honda и гигант ТЭК — компания Enel Group. Snake останавливает процессы GE Proficy и GE Fanuc Licensing, Honeywell HMIWeb, FLEXNet Licensing Service, Sentinel HASP License Manager, ThingWorx Industrial Connectivity Suite;
- Апрель 2020 г. Атака на португальскую энергетическую компанию. Energias de Portugal представляет собой транснациональный холдинг, который занимается производством, распределением по сетям и сбытом электроэнергии, а также закупками, доставкой и сбытом природного газа. Является самой крупной производственной компанией в Португалии, а также одним из крупнейших производителей ветряной электроэнергии в мире;
- Декабрь 2020 г. Атака на SolarWinds. Злоумышленники получили доступ к системе сборки SolarWinds Orion и добавили бэкдор в файл SolarWinds.Orion.Core.BusinessLayer.dll. В настоящее время известный список организаций, пострадавших от атаки, включает: FireEye; Министерство финансов США; Национальное управление по телекоммуникациям и информации США (NTIA); Государственный департамент США; Национальные институты здоровья (NIH) (часть Министерства здравоохранения США); Министерство внутренней безопасности США (DHS); Министерство энергетики США (DOE); Национальное управление ядерной безопасности США (NNSA); Некоторые штаты США (конкретные штаты не разглашаются); Microsoft; Cisco;
- Май 2021 г. Атака на американского производителя ядерного оружия. Американская компания Sol Oriens, связанная с производством ядерного оружия, подверглась атаке шифровальщика REvil;

Текущее состояние кибербезопасности объектов КИИ. Отечественные спецсужбы характеризуют уровень кибератак на РФ, как «критический». Главным вызовом 2022 г. для сферы информационной безопасности в России стал беспрецедентный рост вредоносной киберактивности.

Рис. 1. Организации, подвернувшие кибератакам

Общее количество кибератак в России по итогам первого полугодия 2022-го в сравнении с тем же периодом прошлого года выросло в 15 раз, сообщила компания StormWall рис.1.Самыми атакуемыми отраслями стали финансовый сектор (32% от общего числа атак), ритейл (14%), логистическая сфера (10%), страховая отрасль (8%) и государственный сектор (18%). Также DDoS-атакам подверглись образовательный сектор (7%), сфера развлечений (5%), туристическая индустрия (4%) и другие отрасли (2%) [8]. Наибольшее количество кибератак (92%), совершаются высокопрофессиональными злоумышленниками., векторы атак направлены на объекты КИИ. Чаще всего внимание хакеров с высокой квалификацией - кибернаемников и проправительственных группировок привлекают государственные учреждения, предприятия энергетики, промышленности и ВПК. Возросший хактивизм, DDoS, попытки взлома, проникновение внутрь сетей, финансовый и репутационный ущерб, это основные киберугрозы сегодняшнего дня.

Координатором по компьютерным инцидентам от государства выступает НКЦКИ в задачи которого входит анализ информации, получаемой от субъектов ГосСОПКА, взаимодействие с субъектами КИИ, осуществление обмена информацией о новых кибератаках, рассылка уведомлений об угрозах и способах противодействия им. НКЦКИ приводит еженедельную статистику по количеству кибератак на объекты КИИ. По мнению специалистов атаки, которые проводятся из разных стран, четко скоординированы рис.2.

Рис. 2. Результаты деятельности НКЦКИ

Источником [9] названы самые опасные киберпреступные группировки:

1. DarkSide- впервые о группировке стало известно в августе 2020 года. Целями преступников выступают крупные компании, сервисы которых специально взламываются для нарушения работы, что повышает вероятность получения выкупа;

2. REvil - приобрели известность после атаки на системы крупнейшего в мире производителя мяса JBS. В итоге корпорация выплатила хакерам $11 млн.

В связи с текущей ситуацией приняты государственные решения, направленные на реализацию мер по обеспечению информационной безопасности наиболее значимые на наш взгляд следующие: Президентом РФ подписан Указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Во исполнения данного указа ФСТЭК разработала новую методику оценки степени информационной

безопасности в госорганах и организациях с госучастием, а также в компаниях, обладающих объектами КИИ. Методика отражает основные показатели: организация и управление защитой информации; внедрение мер защиты; поддержка ее уровня (например, мониторинг и реагирование компании на инциденты, управление уязвимостями).

Минцифры РФ опубликовало типовое техническое задание на выполнение работ, по оценке уровня защищённости информационной инфраструктуры. Для этого необходимо решить следующие задачи:

- выявление и консолидация стратегических рисков (недопустимых событий) информационной безопасности;
- выявление уязвимостей информационной инфраструктуры, которые могут быть использованы внешними и внутренними нарушителями для несанкционированных действий, направленных на нарушение свойств конфиденциальности, целостности, доступности обрабатываемой информации, а также технических средств обработки информации, в результате которых может быть нарушен их штатный режим функционирования, что приведёт к недопустимым событиям;
- выявление недостатков применяемых средств защиты информации и программных продуктов, а также оценка возможности их использования нарушителем;
- проверка практической возможности использования уязвимостей (на примере наиболее критических);
- получение оценки текущего уровня защищённости на основе объективных свидетельств;
- разработка маршрутной карты модернизации информационной инфраструктуры.

Кроме того, будет учитываться обучение персонала и осведомленность сотрудников в вопросах кибербезопасности. [10].

В свою очередь Министерство цифрового развития, связи и массовых коммуникаций РФ разослало 58 ключевым госкорпорациям письмо, в котором указало о необходимости провести аудит информационной безопасности. Кроме того, во всех российских регионах созданы штабы по информационной безопасности.

Правительство РФ установило требования к топ-менеджерам, ответственным за кибербезопасность в государственных органах и корпорациях.

В настоящее время Минцифры разрабатывает реестр недопустимых событий в информационной безопасности для госструктур и объектов КИИ, для этого учреждения и предприятия должны провести анализ защищенности и представить отчет в правительство. Все вышеперечисленные меры будут не достаточны без повышения уровня ответственности руководителей учреждений и организаций.

Как показано на рис.3 государственные учреждения во II квартале 2022 года столкнулись с наибольшим количеством кибератак среди организаций: и их доля от общего числа атак возросла на 2 п. п. по сравнению с предыдущим кварталом. Источник [11] констатирует факт, что кибератаки на госучреждения в 59% случаев приводили к нарушениям основной деятельности, что, в свою очередь, может привести к ущербу интересам государства (65%).

Решения для обеспечения безопасности объектов КИИ. Надежная защита данных, безопасность ИТ-инфраструктуры, в том числе объектов КИИ, сохранение штатного функционирования бизнес-процессов и соблюдение требований законодательства — обязательные условия устойчивого развития современного бизнеса. Чтобы выполнить эти условия, недостаточно просто применять защитные решения — необходимо обладать всей полнотой информации о состоянии безопасности комплексной ИТ-инфраструктуры и подготовить инструменты для своевременного выявления и нейтрализации возможных угроз. Разрозненные и неинтегрированные средства защиты малоэффективны против хорошо скоординированных современных атак в условиях сложной инфраструктуры.

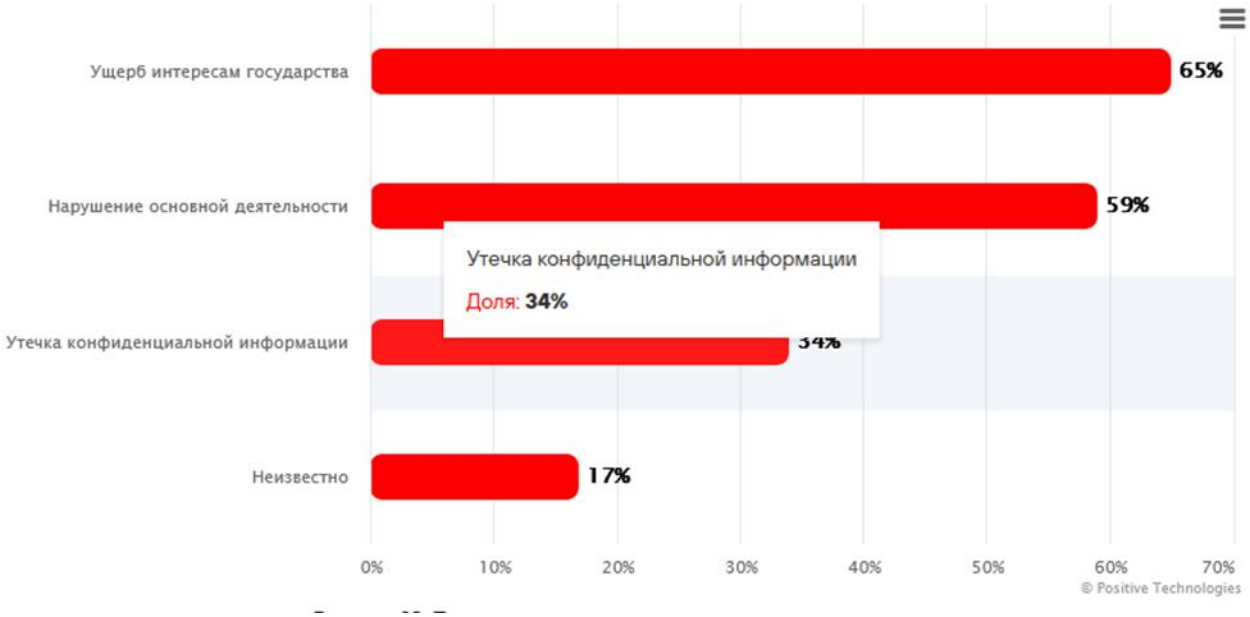

Рис.3. Кибератаки на государственные учреждения

Решение «Единая платформа безопасности», была разработана Лабораторией Касперского для реализации требований ФЗ №187 «О безопасности критической информационной инфраструктуры».

Рис.4. Схема реализации единой платформы кибербезопасности

Kaspersky Unified Monitoring and Analysis Platform (KUMA) — один из ключевых компонентов на пути к реализации единой платформы кибербезопасности. Решение обеспечивает гибкий комплексный подход к противодействию сложным угрозам и целевым атакам, объединяет решения «Лаборатории Касперского» в единую экосистему, например, в XDR-платформу Kaspersky Symphony XDR, которая состоит из взаимосвязанных и взаимодополняющих друг друга продуктов, легко встраивается в существующую ИТ и ИБ-инфраструктуру и помогает подойти комплексно к вопросу соответствия требованиям внешних регулирующих органов[12].Схема функционирования единой платформы кибербезопасности представлена на рис.4.

Реализаций требований законодательства в данном продукте реализуется в несколько этапов:

- Первичный сбор данных;
- Проведение категорирования;
- Разработка мероприятий по взаимодействию со ФСБ России.

Данное решения помогут организациям соответствовать требованиям законодательства РФ в области безопасности КИИ, в том числе к построению центров ГосСОПКА.

Компания Positive Technologies также активно представляет на рынке решение для безопасности объектов КИИ, которые позволяют выполнить основные законодательные требования по защите значимых объектов КИИ, предотвращать и выявлять атаки и автоматизировать взаимодействие с ГосСОПКА.

При многоуровневой инфраструктуре, как показано на рис.5 продукты Positive Technologies выстраиваются в иерархию. На нижних уровнях, где нет компетентных специалистов по ИБ или недостаточен объем бюджета на ИБ, устанавливаются сенсоры для сбора и передачи информации в крупные филиалы. Специалисты по ИБ в филиалах выявляют и расследуют атаки и отправляют данные об инцидентах в головную организацию, где консолидируется информация об инцидентах во всей компании и осуществляется взаимодействие с главным центром ГосСОПКА [12]. Кроме того, данное решение позволяет обеспечить хранение сырого трафика, сбор детальной информации об IT-активах, реконструкцию сессий, ретроспективный анализ и возможность детализации данных об атаках, что в свою очередь позволяет эффективно провести расследование.

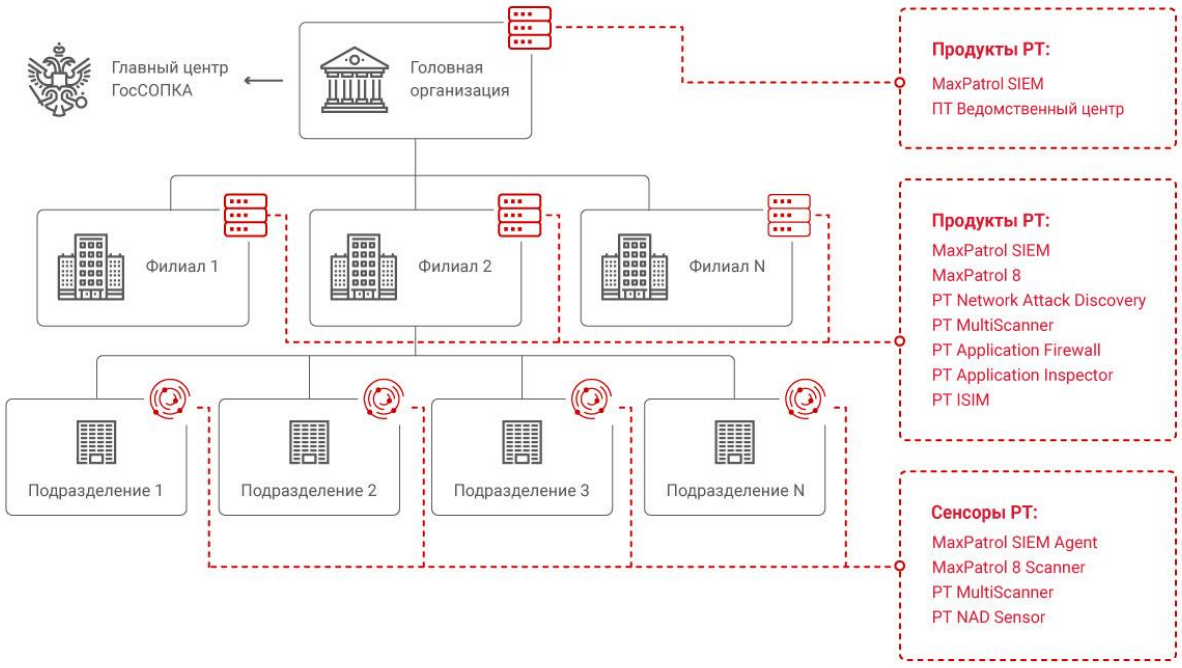

Рис.5. Схема архитектурного решения при многоуровневой инфраструктуре

Анализируя вышеизложенное можно сказать, что отечественные разработчики в настоящее время представляют для субъектов КИИ готовые решения которые позволяют создать комплексную систему защиты, позволяющую обеспечить требуемый уровень информационной безопасности.

Выводы. Актуальность информации и выводы, приведенные в статье, очевидны. С учетом высокой степени киберугроз в отношении объектов КИИ в настоящее время, необходимо обеспечить комплексный последовательный подход к созданию систем безопасности, необходимо использовать надежные и комплексные системы защиты отечественных производителей. Неукоснительного исполнения требования регуляторов в сфере защиты информации и обеспечения устойчивого функционирования объектов КИИ.

Надеемся, что изложенные в статье информация может быть полезна аспирантам преподавателям, ведущим научную и педагогическую деятельность в предметной области, а также возможность практического применения материала статьи специалистами по защите информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://www.kommersant.ru/.
2. https://interaffairs.ru/jauthor/material/2379?ysclid=lb8ugvusth858101242.
3. https://dlp.cnews.ru/articles/2022-06-20_kiberbezopasnost_kii_ot_teorii.
4. https://www.tadviser.ru/index.php.
5. https://blog.avast.com/ru.
6. https://www.it-world.ru.
7. https://en.wikipedia.org.
8. https://rdc.grfc.ru/.
9. https://www.gazeta.ru/.
10. https://d-russia.ru/.
11. https://www.ptsecurity.com/ru-ru/about/.
12. https://www.ptsecurity.com/ru.
13. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / — Екатеринбург: Изд-во Урал.ун-та, 2019. — 204 с.
14. С.И. Макаренко. Фрагмент монографии Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. — СПб., 2017.
15. Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".
16. Указ Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации".

REFERENCES

1. https://www.kommersant.ru/
2. https://interaffairs.ru/jauthor/material/2379?ysclid=lb8ugvusth858101242
3. https://dlp.cnews.ru/articles/2022-06-20_kiberbezopasnost_kii_ot_teorii
4. https://www.tadviser.ru/index.php
5. https://blog.avast.com/ru
6. https://www.it-world.ru
7. https://en.wikipedia.org
8. https://rdc.grfc.ru/
9. https://www.gazeta.ru/
10. https://d-russia.ru/
11. https://www.ptsecurity.com/ru-ru/about/
12. https://www.ptsecurity.com/ru

13. Vostretsova E.V. Fundamentals of information security: a textbook for university students / — Yekaterinburg: Ural Publishing House.un-ta, 2019. — 204 p

14. S.I. Makarenko. Fragment of the monograph Information warfare and electronic warfare in the network-centric wars of the beginning of the XXI century. — St. Petersburg, 2017.

15. Decree of the President of the Russian Federation No. 250 dated 01.05.2022 "On additional measures to ensure Information security of the Russian Federation".

17. Decree of the President of the Russian Federation

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. Особенности кибератак на объекты критической информационной инфраструктуры в современных условиях // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2022. – №4(16). – С. 56-66 – DOI: 10.26731/2658-3704.2022.4(16).56-66 – Режим доступа: http://ismm-irgups.ru/toma/416-2022, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 23.12.2022).

For citations

Seryodkin S.P. Review of regulatory and legal acts to ensure the security of critical information infrastructure: // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2022. No. 4(16). P. 56-66. DOI: 10.26731/2658-3704.2022.4(16).56-66 [Accessed 23/12/22].