КИБЕРУЧЕНИЯ: ЗАРУБЕЖНЫЙ ОПЫТ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Метельков А. Н.[1]

Ключевые слова*: киберинциденты, киберугрозы, кибербезопасность, моделирование, защита информации, информационно-коммуникационные технологии, координация.*

Аннотация.

Цель работы: на базе анализа материалов о киберучениях, проводимых в США и других странах, выделить пути совершенствования методов и средств обеспечения информационной безопасности.

Метод исследования: комплексный теоретико-сравнительный анализ и обобщение опыта проведения в США и других странах исследовательских учений в киберпространстве, проводимых для обеспечения корпоративной безопасности. Применение при планировании киберучений моделирования сценариев учебной обстановки как эффективного метода комплексного исследования системы реагирования на кибератаки и защиты государственных и частных ресурсов, систем и сетей в условиях сложности и многоплановости кибератак, описание воздействия которых на сложную взаимозависимую инфраструктуру ряда секторов деятельности современного человека с использованием математических моделей весьма сложно. Исследование зарубежных подходов показывает актуальность экспериментальных методов имитационного моделирования кибератак на чувствительную информационную инфраструктуры различных отраслей экономики и государственного управления.

Результаты: раскрыто понятие кибербезопасности и выделены особенности организационно-технических методов и средств ее обеспечения в США и других странах. Проанализирован зарубежный опыт моделирования кибератак в ходе крупномасштабных киберучений, который возможно использовать при отработке сценариев кибератак в отечественных технологиях киберполигонов по подготовке специалистов в условиях бурного развивающихся технологий и возрастающих рисков кибербезопасности. На основе обобщения опыта предложены имитационная модель учебного сценария реализации киберугроз и общая модель организационной структуры киберучений.

DOI: 10.21681/1994-1404-2022-1-51-60

Введение

Уязвимость критической инфраструктуры (КИ) для внешних и внутренних кибератак возрастает по мере усиления ее зависимости от информационных технологий (ИТ). 14 января 2022 г. на официальном сайте ФСБ России в Интернете была размещена информация о пресечении организованной преступной деятельности 14 членов сообщества «REvil» в ходе реализации сведений компетентных органов США о причастности его лидера к посягательствам на информацию иностранных высокотехнологичных компаний путем шифрования информации и вымогательства денег за ее расшифрование с использованием вредоносных программ. В числе таких атак могут быть и кибертеррористические, создающие угрозы экономике страны, общественным работам, системам связи, компьютерным сетям и другой критически важной инфраструктуре. В обстановке пандемии COVID-2019 кибератаки, нарушающие телекоммуникационные возможности, могут серьезно повлиять на работу службы скорой медицинской помощи и пожарных частей, привести к задержке реагирования на чрезвычайную ситуацию, создать реальную угрозу жизни и здоровья сотням людей. В этих условиях для объектов сферы здравоохранения и фармацевтической промышленности актуальной задачей является способность выполнения целевой функции [1]. Поэтому данную ситуацию также можно рассматривать как актуальную проблему защиты от посягательств на основные конституционные ценности и жизненно важные интересы человека, общества и государства.

В ряде государств после возникновения пандемии коронавируса усилились опасения по поводу кибербезопасности, что побудило государственные и частные организации перенести часть своей деятельности в Интернет. В связи с этим возникли новые реальные и

[1] ***Метельков Александр Николаевич,*** *кандидат юридических наук, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, г. Санкт-Петербург, Российская Федерация.*

E-mail: metelkov5178@mail.ru

потенциальные угрозы, расширился спектр кибератак [2, 3, 4] на критически важную и общественно значимую инфраструктуру, что требует обеспечения устойчивости функционирования государственных и частных корпоративных систем и сетей. Обеспечению их устойчивости способствует осуществление моделирования сценариев киберучений — комплекса взаимосвязанных и взаимозависимых действий и операций их участников в киберпространстве.

Технологии киберполигонов [5, 6] позволяют обучать персонал [7] противодействовать этим угрозам. В России такие технологии с конца 2019 г. стали системно разрабатываться и с 2020—2021 гг. внедряться в образовательный процесс. В учебных заведениях путем применения новых технологий принимаются меры по сокращению разрыва между распространением дистанционных методов обучения с использованием территориально-распределенных информационных систем (ИС) и недостаточным уровнем их защиты. В 2021 г. с использованием технологий киберполигона в Санкт-Петербургском университете Государственной пожарной службы (ГПС) МЧС России совместно с компанией «ИнфоТеКС» проведены занятия с применением ролевого обучения (с выделением групп мониторинга и реагирования), направленные на выработку мер борьбы с кибератаками на систему управления в чрезвычайных ситуациях. В США обучающие платформы Cyber-Ranges (CR) предоставляют возможности по нейтрализации кибератак [8, 9].

Глобализация приводит к усилению взаимосвязанности государственных и частных структур. Повышенная связанность информационных и киберфизических систем создает дополнительные риски в сфере обеспечения информационной безопасности, поэтому управление системным риском требует сотрудничества и обмена информацией, побуждает к поиску новых методов и средств мониторинга, обнаружения и нейтрализации киберугроз, минимизации их последствий. Системные риски отличаются взаимосвязанностью, распространяются в коррелирующих системах, преодолевая границы ситуационной осведомленности или оперативного контроля. Риски особенно опасны в электроэнергетике, атомной промышленности, финансах, госуправлении и др. Системный риск начинается с распределенного уязвимого состояния, которое изменяется по мере усложнения социальных и технологических систем. Источником риска может быть зависимость взаимосвязанных систем от информационных и коммуникационных технологий, поддерживающих расширяющийся спектр приложений. Системный риск может использоваться злоумышленником для дестабилизации или разрушения критических функций. Отдельные инициирующие инциденты накапливаются и приводят к нежелательным эффектам, которые усиливаются с нарастающим ущербом. В результате возникают каскадные эффекты, способные затронуть как отдельные корпоративные информационные системы (ИС), так и цифровую инфраструктуру одного или нескольких секторов экономики. Нападения происходят из различных источников и включают атаки типа «отказ в обслуживании», распространение вредоносных вирусов, которые заражают сеть компании и используют бреши в безопасности для доступа к конфиденциальной информации, а также поддельные электронные письма с запросом конфиденциальных данных от ничего не подозревающего сотрудника, фишинг. Определение мотивированного нарушителя кибербезопасности и вектора атаки при моделировании угрозы во время учений стимулирует активную работу обучаемых [10, 11]. Моделирование фишинговой атаки включает обнаружение и блокирование системой обнаружения вторжений и противодействия компьютерным атакам, антивирусным программным обеспечением (ПО) — содержащих вредоносный код электронных сообщений, прочтения их пользователями компьютеров, а также блокирования «передачи сообщений на серверы злоумышленников» [12]. Векторы атаки выстраиваются с применением средств компьютерной автоматизации. Для этого могут разрабатываться полные графовые модели деструктивных кибервоздействий на сетевую инфраструктуру сложных объектов критического назначения [13, с. 18]. Несмотря на множество методов моделирования угроз безопасности информации (УБИ) и признанных реестров или баз данных уязвимостей ПО [14, с. 53], различных систем классификации и оценки критичности уязвимостей, нередко авторами при разработке методики выявления взаимосвязей между обнаруженными уязвимостями ИС и УБИ в качестве основного источника сведений об угрозах и уязвимостях используется только Банк данных УБИ ФСТЭК России [16, с. 271]. При таком подходе к оценке неактуальности «угрозы несанкционированного восстановления удалённой защищаемой информации» для ИС со стороны допущенных к информации пользователей обосновывается предположение о нецелесообразности действий по восстановлению и так известной нарушителю информации [17, с. 29] и остается без внимания возможность активизации таким способом заранее внедренного вредоносного программного кода.

Российские подходы к определению вероятных объектов кибератак и оценке способов реализации УБИ отражены в Методике ФСТЭК России [18]. Исследование зарубежных и российских подходов к моделированию УБИ в числе проблем в подготовке решений позволяет выделить несовершенство экспертных методов, а также большой объем сложно структурируемых данных для моделирования. Преодолеть эти трудности помогают экспериментальные методы, основанные преимущественно на моделировании (CyberVAN) и эмуляции (Testbed, INSALATA, SoftGrid и LARIAT), а также на методах наложения и демонстрации сценариев. В ходе учений нередко имитируется многосвязная сеть (центры управления, центры обработки данных) и атаки на системы информационных и операционных технологий через Интернет (SQL-инъекции, отключение Apache, уничтожение системы NMS, перехват дампа

Рис.1. Общая схема осуществления кибератаки

базы данных через протокол передачи файлов, программы-вымогатели, DDoS, SCADA и др.).

Бурное внедрение информационных технологий (ИТ) во многие сферы человеческой деятельности актуализирует изучение, обобщение и анализ зарубежного опыта для его учета в совершенствовании отечественных систем реагирования на киберинциденты.

Моделирование учебной обстановки методом имитации кибератак

С каждым годом многошаговые скоординированные распределенные кибератаки со сложной организацией, реализацией и множеством целей изменяются, проводятся все чаще и изощреннее. На этапе вторжения кибератаки обычно обнаруживают с использованием сигнатурных, поведенческих, комбинированных и иных методов [15]. В современном ландшафте киберугроз на первый план выдвигается создание интеллектуальных средств защиты, позволяющих обнаруживать целевые атаки на начальных этапах их реализации [15, с. 2].

Отличительной чертой КИ является ее функционирование посредством взаимодействия с мировым киберпространством, что формирует дополнительные уязвимости для возможной их эксплуатации при оказании деструктивных воздействий на государственные и муниципальные системы, объекты экономики без непосредственного проникновения на территорию государства и объявления санкций. В киберпространстве возможно дистанционное управление и перевод в режим функционирования в интересах нарушителя вплоть до сбоев в работе автоматизированных ИС и отключения объектов КИ. Особенно опасно переключение объекта в критический режим функционирования, приводящий к его разрушению [12, 4—6].

При проведении учений в киберпространстве моделирование кибератак является важным этапом их подготовки. Моделирование основано на формализации логической цепочки: взаимодействия множеств выявленных уязвимостей ПО, релевантных угроз, вероятных сценариев реализации угроз, возможных киберфизических последствий количественной оценки рисков нарушения кибербезопасности [20]. Общая схема кибератаки представлена на рис. 1.

В общем случае при формализации киберучений вычисляется функция F, то есть выявляется связь между показателями эффективности V защиты критической информационной инфраструктуры, исходными данными D на момент кибератаки и переменными X при известных значениях факторов W, характеризующих риски информационной безопасности:

$$V = F\,(D, X, W) \quad (1)$$

Множество X характеризует ряд известных и неизвестных кибератак и состоит из n элементов $X = \{x_1, x_2, x_3, \ldots x_n\}$, где каждый из элементов x_i $(i=1\ldots n)$ определяется конкретным видом атаки, инициируемой руководством киберучений согласно плану имитации кибератак в определенный момент времени t_j последовательно, одновременно или последовательно-параллельно. В учебных технических задачах для обеспечения безопасности реальных процессов вводится ряд ограничений, что облегчает процесс формализации.

С применением технологий киберполигона одним из экспериментальных методов с помощью имитации реальных инцидентов безопасности и динамики угроз является создание реалистичных сценариев кибератак на целевые системы в среде моделирования, облегчая обучение ИТ-специалистов в выборе наиболее подходящих ответов. Сценарии представляют собой в основном смоделированные или эмулированные сети, тра-

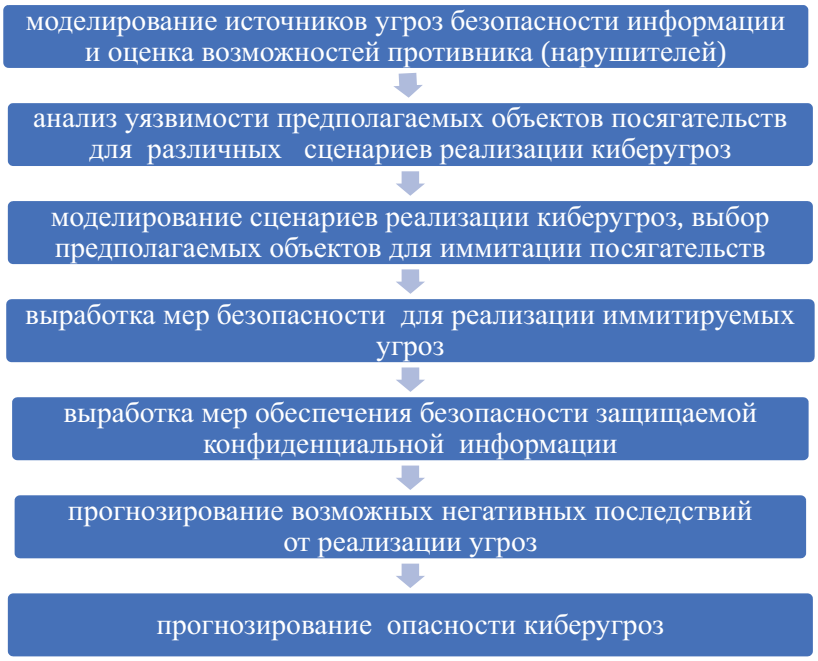

Рис. 2. Имитационная модель учебного сценария реализации киберугроз

фик в которых наполняется потенциальными угрозами в компьютерных сетях различного типа (PAN, LAN, MAN, WAN). Программное и аппаратное решение реализуется с использованием виртуальных машин, контейнеров или песочниц (Sandbox). Метод имитационного моделирования кибератак можно определить в качестве методологического средства, способствующего познанию результатов реализации УБИ на информационную инфраструктуру целостной системы или отдельные ее элементы через воздействие на информацию, ИТ и технические средства.

Целями моделирования на учениях является поиск оптимальных решений по системному реагированию на запланированные по времени, как правило, внешние воздействия кибератак, а также оценка эффективности принятых решений по нейтрализации киберугроз и изучение чувствительности сложной взаимозависимой информационной инфраструктуры к влиянию различных УБИ. В процессе моделирования УБИ выявляются условия и факторы, подрывающие безопасность обрабатываемой информации, приводящие к нарушению функционирования систем и сетей.

Имитационное моделирование направлено на получение новых знаний об информационной безопасности в заранее определенных условиях при наличии исходной информации об объектах деструктивного воздействия на элементы исследуемой информационной инфраструктуры в создаваемой учебной обстановке. Модель может включать систематизированный перечень УБИ, исходящих из источников, имеющих антропогенный, техногенный или стихийный характер и воздействующих на характерные уязвимости ИС. Процесс моделирования подразумевает выработку вводных для обучаемых, которые после обнаружения признаков инцидента принимают решения по нейтрализации угроз и адаптации систем безопасности к изменившейся обстановке.

Ввиду сложности территориально-распределенной инфраструктуры, особенностей ИТ обработки данных, использования незащищенных каналов связи потенциально увеличивается количество УБИ, что требует для их моделирования использования автоматизированных методик определения актуальных из них [14, с. 53]. Процесс моделирования УБИ предлагаем представить в виде модели сценария инициирования киберугроз (рис. 2).

Сигналы об угрозах, отдаваемые руководством киберучения, дают представление о возникающих проблемах в ландшафте угроз, инициируют необходимость углубленного исследования новых вредоносных программ и их вариантов, эксплойтов нулевого дня, целевых систем и критических уязвимостей. Для противодействия атакам и защиты информационных активов организациям необходимо своевременно обнаруживать и корректировать в реальном масштабе времени состояние безопасности в отношении обнаруженных атак на их расширяющейся поверхности. Среди тактик и приемов в действиях нарушителей зарубежными специалистами выделяются:

- целевой фишинг для получения первоначального доступа к компьютерной сети организации-цели до перехода к сети операционных технологий (ОТ);
- развертывание серийных программ-вымогателей для шифрования данных для воздействия в сетях ИТ и ОТ;
- подключение к программируемым логическим контроллерам (ПЛК) с доступом в Интернет, не требующим аутентификации для начального доступа;
- эксплуатация часто используемых портов и стандартных протоколов уровня приложений для свя-

зи с контроллерами и загрузки измененной логики управления;
- использование ПО для проектирования и загрузки программ;
- изменение логики управления и параметров на ПЛК.

Выработка рекомендаций помогает организациям понять жизненный цикл УБИ, выбрать технологии и методы защиты данных.

Возможности обучения в реальных сетях ограничены, что связано с потенциальным деструктивным влиянием тренингов на операционную деятельность предприятий и организаций, затратами людских, финансовых и иных ресурсов. Поэтому для создания реалистичной учебной среды используют методы моделирования сценариев кибератак при состязательной атаке и активной защите. Физические, эмулированные и смоделированные модели позволяют углубить понимание и изучить социально-технические системы кибербезопасности. Имитационные модели предоставляют средства для изучения сложных взаимодействий и изменений внутри системы в течение определенного времени, включая влияние социальных субъектов на функционирование аппаратно-программных и программных средств.

Анализ зарубежного опыта проведения киберучений

В последние годы кибераторы продемонстрировали готовность к злонамеренной кибератакивности против КИ путем использования доступных в Интернете ресурсов ОТ.

Кибербезопасность как постоянно расширяющаяся и обостряющаяся проблема охватывает сочетание физических, программных и человеческих систем. Для выработки учебной платформы в мире организуется ряд мероприятий. Тренинги играют ключевую роль в формировании и проверке организационной и технической готовности для отражения реальных кибератак. При поддержке Центра кибербезопасности Всемирного экономического форума и Интерпола компанией BI.ZONE (Sber Ecosystem) и ПАО «Сбербанк» ежегодно проводится онлайн-мероприятие Cyber Polygon, объединяющее международные компании для обучения необходимым компетенциям, обмена опытом. С 2010 г. в Европе каждые два года проводятся киберучения Cyber Europe (CE), организуемые Агентством Европейского союза по кибербезопасности (ENISA). Пандемия COVID-19 высветила необходимость повышения безопасности в киберпространстве в связи с увеличением в Интернете личных и профессиональных контактов. Киберпреступники воспользовались этой ситуацией, нацелившись на систему здравоохранения, предприятия электронной коммерции и электронных платежей. Не случайно в сценарий CE 2022 включены технические инциденты, которые могут быть исследованы с помощью криминалистического анализа и анализа вредоносных программ. Для проверки планов антикризисного управления здравоохранением и обеспечения непрерывности бизнеса по сценарию учений отдельные инциденты перерастут в серьезный кризис на местном, национальном и европейском уровнях.

Комплексному обучению кибербезопасности технических специалистов в США способствует программа Cybersecurity Defense Initiative (CDI), бесплатно проводятся курсы для ее освоения. Курсы «Комплексная защита кибербезопасности» (CCD) и «Специалист оперативного реагирования по кибербезопасности» (CFR) сертифицированы Министерством внутренней безопасности США (DHS). Секретная служба США (USSS) с участием правоохранительных органов и партнеров из частного сектора проводит учения по реагированию на инциденты кибербезопасности и отработку стратегий смягчения их последствий методом виртуального моделирования атак с использованием программ-вымогателей и криптовалюты. На семинарах FEMA Region III по кибербезопасности осуществляется презентация плана реагирования на инциденты, проводятся штабные тренировки. Для сотрудников федерального правительства и других органов власти, государственных подрядчиков доступна сформированная на бесплатной онлайн-платформе виртуальная учебная среда кибербезопасности FedVTE, управляемая DHS. Среда, доступ в которую осуществляется по запросу, содержит модули мониторинга инцидентов, управления рисками и анализа вредоносных программ. Федеральные департаменты используют системы обнаружения вторжений Einstein и US-Cert. Для защиты от атак вредоносного ПО при подключении к федеральным системам DHS принимает меры по сокращению числа точек доступа в Интернет.

Модель актуальных киберугроз может разрабатываться для отдельных систем, сетей и информационно-телекоммуникационной инфраструктуры, на которой они функционируют. Угрозы, связанные интерфейсами взаимодействия с системами и сетями, инициируются при отработке учебных эпизодов доведением вводных. Процесс моделирования УБИ включает определение возможных негативных последствий от их реализации, условий реализации и источников угроз, оценку возможностей злоумышленников, сценариев реализации угроз и опасности кибератак. Цели и сценарии осуществления угроз, прогнозируемые последствия от их реализации уточняются экспертным методом.

Критически важные системы связи и энергоснабжения считаются настолько значимыми для США, что их выведение из строя или разрушение может оказать пагубное воздействие на различные виды безопасности: национальную [21], экономическую, общественную. Официальные лица признают устранение последствий преднамеренных кибератак на критически важные инфраструктуры дорогостоящим для страны [20, 22]. Поэтому для решения системных проблем необходимы определение приоритетов, разработка общей терминологии, организация реагирования на инциденты.

Имитационные киберучения

Суть киберучений заключается в проверке реагирования на моделируемые угрозы. Для анализа применения метода моделирования при проведении масштабных киберучений целесообразно рассмотреть и обобщить опыт США. В ходе стратегических учений в создаваемой обстановке с соблюдением мер безопасности разработчиками предлагались сценарии кибератак, максимально приближенные к реальным и потенциальным рискам. На основе итогов учений DHS разрабатываются национальные киберучения и программа поддержки планов реагирования на киберугрозы.

Одним из основных инструментов проверки эффективности обеспечения кибербезопасности в США служат масштабные учения под названием Cyber Storm (CS), проводимые каждые два года [23]. Учения являются частью программы Агентства DHS по кибербезопасности и безопасности инфраструктуры (CISA), направленной на изучение процессов комплексного реагирования государственных, частных и международных партнеров на масштабные кибератаки, а также на оценку и повышение уровня подготовки к нейтрализации киберугроз, совершенствование процедур и обмена информацией, координацию и принятие решений [24]. Новые знания способствуют совершенствованию способов реагирования на инциденты согласно Национальному плану реагирования на киберинциденты (NCIRP).

Впервые национальные киберучения CS I были проведены 6—10 февраля 2006 г. CS II проведены в 2008 г., CSIII — в 2010 г., CS IV — в 2012 г., CS V — в 2016 г., CS VI — в 2018 г. и CS 2020 — в 2020 г. Если в CS I по приглашению CISA было привлечено более 100 государственных и частных агентств, ассоциаций и корпораций, всего 500 человек из пяти стран, то к 2020 г. это число выросло в 20 раз: свыше 2000 участников из 12 стран и свыше 210 партнерских организаций. Учения CS I координировались в рамках национальной программы учений DHS по проверке реакции на кибератаки. В автономной сети без воздействия на реальные ИС моделировалась обстановка в виде крупномасштабного киберинцидента, затронувшего критически важную инфраструктуру энергетики, ИТ, телекоммуникаций и транспорта. В 2008 г. в ходе CS II использовались возможности индивидуального реагирования. Межсекторные атаки создавали условия для скоординированного ответа, побуждали участников к сотрудничеству. Участники получили целостное представление о взаимосвязанном характере киберреагирования, а также о зависимости между киберактивностью, физической инфраструктурой и экономическими последствиями. На учениях CS III моделировалось реагирование на национальном уровне с испытанием координационного центра CISA Central. В число участников вошли 1725 пользователей системы CS III, включая 60 частных компаний, представлявших критические секторы инфраструктуры (ИТ, связь, электроэнергетика, химическая промышленность, транспорт), и координационных органов — центров обмена и анализа информации (ISAC). Учения с элементами реальной киберугрозы позволили проверить версию NCIRP и работу CISA Central. Условный противник действовал как слабо организованная зонтичная организация, объединенная для проведения целевых атак в результате компрометации системы доменных имен (DNS) и цепочки доверенных лиц в Интернете. Целью противника была попытка поставить под сомнение способность участников работать в доверенной среде, выполнять транзакции и поддерживать критически важные функции. Учения CS VI предоставили площадку для моделирования реагирования на крупномасштабную скоординированную кибератаку на критически важную инфраструктуру путем повышения готовности и возможностей реагирования за счет применения политик, процессов и процедур. На учениях CS VI в течение недели был смоделирован киберкризис национального и международного значения для проверки реагирования на инциденты, затрагивающие нетрадиционные ИТ-устройства, с привлечением новых участников из критически важных отраслей промышленности, включая автомобильную. Учебные задачи были сфокусированы на оценке и улучшении возможностей реагирования на эскалацию киберинцидентов, развитие государственно-частного партнерства в 16 секторах критической инфраструктуры. Участники наблюдали за потенциальным воздействием атаки и отрабатывали скоординированный ответ. Учения подтвердили важность расширения экосистемы и реагирования на киберинциденты, охватывающие все типы потенциально уязвимых в киберпространстве систем, технологий и IoT устройств (системы отопления, вентиляции и кондиционирования). CS V в марте 2016 г. обеспечили возможности усовершенствования механизмов координации для отраслевых ISAC и организаций по обмену и анализу информации (ISAO), завершили серию киберучений DHS на национальном уровне. Учения объединили более 1000 участников, включая секторы розничной торговли и здравоохранения. Основной сценарий был сосредоточен на трех базовых критически важных для архитектуры Интернета службах, обеспечивающих доступ к веб-страницам только легальным пользователям. Замыслом учений предполагалось, что две группы обозначения противника на уровне государств будут работать через аффилированных лиц и обмениваться инструментами, способными эксплуатировать уязвимости DNS, CA и BGP для атак на выбранные цели. Спектр атак включал перехват трафика (MITM), имитацию веб-сайтов, расширенные фишинговые кампании и множественное заражение вредоносными программами и программами-вымогателями. Один из сценариев был связан с потерей сертификата аутентификации. По замыслу учения хакерам удалось скопировать сертификаты центра сертификации и с использованием их копий выдать себя за законных участников сети, в которой они не были зарегистрированы. Другие сценарии включали взлом системы доменных имен.

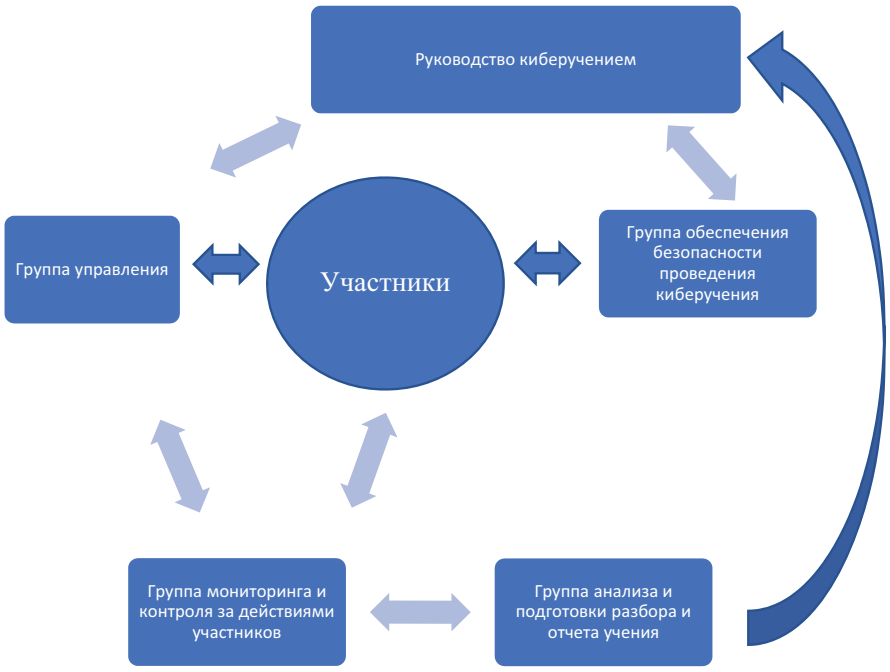

Рис.3. Модель организационной структуры киберучений

10—14 августа 2020 г. учения CS 2020 подтвердили, что усилия государства и частных субъектов по развитию рабочих отношений, формализации процедуры обмена информацией на основе единого понятийного аппарата, а также по созданию структур управления и контроля до инцидента способствуют повышению качества информационного взаимодействия непосредственно во время реагирования на киберинциденты, наращиванию коллективной способности отражения кибератак. В конечном итоге скорость и эффективность обмена информацией при реагировании на инциденты влияет на способность респондентов минимизировать последствия и своевременно отреагировать на событие.

В результате исследования зарубежного опыта, проведенного анализа научных публикаций и опубликованных DHS отчетов по киберучениям в условиях нарастания опасности кибератак разработана модель организации киберучений (см. рис. 3).

Автором на основе исследования зарубежного опыта проведения киберучений по противодействию киберугрозам в отношении защищаемых информационных ресурсов в условиях усложнения взаимосвязей и взаимозависимости ИС обоснована актуальность решения научной задачи оценки рисков нарушения и сделаны следующие выводы.

Выводы

1. Проведение учений является современной организационно-технологической исследовательской платформой для анализа угроз, информирования участников и заинтересованных лиц и организаций о новых угрозах и их последствиях, тенденциях в развитии с целью принятия упреждающих мер путем совершенствования мер защиты, методов и средств обнаружения и предотвращения кибератак.

2. Учения предоставляют возможность объективного исследования в контролируемой среде прогнозируемых масштабных воздействий на взаимосвязанную и взаимозависимую распределенную информационную и киберфизическую инфраструктуру государства и общества, корпоративных структур и других организаций, а также проверить и оценить их подготовленность к системному реагированию.

3. При обеспечении информационной безопасности в будущем необходимо сосредоточиться на учете корреляции множественных киберинцидентов и коммуникаций, координации и сотрудничестве в реагировании заинтересованных государственных и частных организаций.

4. Анализ угроз и обмена информацией дает возможность специалистам безопасности идентифицировать начальные проблемы, позволяющие организациям инициировать анализ события и обнаружение вредоносных сертификатов и кода вымогателя, защитить свои сети.

5. Разработка и внедрение общей терминологии способствует улучшению координации в сфере обеспечения информационной безопасности, повышению эффективности информационного обмена.

Заключение

Расширение сферы и изощренности кибератак на нетрадиционные ИТ-устройства, операционные ИТ и процессы изменяет характер реагирования на киберинциденты и требует специализированного планирования, поддерживающего наиболее полное представление об

угрозах. Киберучения как высшая форма подготовки специалистов в области информационной безопасности позволяют объективно оценить возможности страны, отдельных отраслей экономики и управления, организаций и участников по реагированию на инциденты с целью дальнейшего развития и адаптации информационной среды к меняющимся рискам и киберугрозам.

Проведенный анализ отчетных материалов об учениях в США показывает, что в случае нейтрализации интегрированных и/или каскадных атак, минимизации и ликвидации их последствий необходимо повышать качество, скорость и координацию реагирования путем совершенствования процессов, инструментов и обучения специалистов. При этом особое внимание надо уделять анализу результатов воздействия сценариев кибератак для определения приоритетов физической, экономической и других видов национальной безопасности.

Для понимания алгоритмов кибератак и обучения специалистов получает широкое распространение имитационное моделирование при реализации разных сценариев угроз. С этой целью на национальном и институциональном уровнях целесообразно создание специализированных учебных платформ, формирование организационной, кадровой, учебно-методической и технологической составляющих для проведения тренингов и учений по кибербезопасности.

Литература

1. Lallie H.S., Shepherd L.A., Nurse J.R.C., Erola A., Epiphaniou G., Maple C., Bellekens X. (2021). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security, 105, [102248]. URL: http://doi.org/10.1016/j.cose.2021.102248
2. Leblanc S.P., Partington A., Chapman I.M., Bernier M. An overview of cyber attack and computer network operations simulation. SpringSim (MMS), 2011, pp. 92–100.
3. Brown B., Cutts A., McGrath D., Nicol D.M., Smith T.P., Tofel B. Simulation of cyber-attacks with applications in homeland defense training. Sensors, and command, control, communications, and intelligence (c3i) technologies for homeland defense and law enforcement II. International Society for Optics and Photonics, 2003, Vol. 5071, pp. 63–71.
4. Kuhl M.E., Sudit M., Kistner J., Costantini K. Cyber-attack modeling and simulation for network security analysis. 2007 Winter Simulation Conference. IEEE, 2007, pp. 1180–1188.
5. Yamin M.M., Katt B., Gkioulos V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. Computers & Security 2019, p. 101636.
6. Radziwill N.M. Virginia cyber range. Software Quality Professional 2017, 19, 46.
7. Aliyu A, Maglaras L, He Y, Yevseyeva I, Boiten E, Cook A, Janicke H. A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. Applied Sciences. 2020; 10(10): 3660. URL: http://doi.org/10.3390/app10103660
8. Singh R, Kumar H, Singla R.K. et al. Internet attacks and intrusion detection system: a review of the literature. Online Inform Rev 2017; 41:171–84.
9. Bures M., Klima M., Rechtberger V., Bellekens X., Tachtatzis C., Atkinson R., Ahmed B.S. Interoperability and Integration Testing Methods for IoT Systems: A Systematic Mapping Study. Software Engineering and Formal Methods; de Boer, F.; Cerone, A., Eds.; Springer International Publishing: Cham, 2020; pp. 93–112.
10. Jason Kick. Cyber Exercise Playbook November 2014. URL: http://www.mitre.org/s/pr_14-3929-cyber-execise-playbook.pdf (дата обращения: 18.01.2022).
11. Gore R, Padilla J, Diallo S. Markov chain modeling of cyber threats. J Def Model Simul 2017; 14:233–44.
12. Добрышин М.М., Закалкин П.В. Модель компьютерной атаки типа «phishing» на локальную компьютерную сеть // Вопросы кибербезопасности. 2020. № 2. С. 17—25.
13. Лаврова Д.С., Зегжда Д.П., Зайцева Е.А. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. 2019. № 2. С.13—20.
14. Миняев А.А. Моделирование угроз безопасности информации в территориально-распределенных информационных системах // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 2. С. 52—65.
15. Japertas S, Baksys T. Method of early staged cyber-attacks detection in IT and telecommunication networks. Elektronika Ir Elektrotechnika, 2018; 24:68–77.
16. Селифанов В.В., Юракова Я.В., Карманов И.Н. Методика автоматизированного выявления взаимосвязей уязвимостей и угроз безопасности информации в информационных системах // Интерэкспо Гео-Сибирь. 2018. № 7. С. 271—276.
17. Воронин В.В., Сухоруков Я.П. Аспекты разработки Частной модели угроз безопасности информации в типовых информационных системах // Вестник ПГУ им. Шолом-Алейхема. 2020. № 1. С. 24—33.
18. Методический документ «Методика оценки угроз безопасности информации», утв. ФСТЭК России 5.02.2021. URL: http://fstec.ru
19. Васильев В.И., Кириллова А.Д., Вульфин А.М. Когнитивное моделирование вектора кибератак на основе меташаблонов CAPEC // Вопросы кибербезопасности. 2021. № 2. С. 2—16.
20. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Автоматизация анализа уязвимостей программного обеспечения на основе технологии Text Mining // Вопросы кибербезопасности. 2020. № 4. С. 22—31.

21. Kavak H., Padilla J.J., Vernon-Bido D., Diallo S.Y., Gore R.J., Shetty S. Simulation for Cybersecurity: State of the Art and Future Directions. Journal of Cybersecurity, Volume 7, Issue 1, 2021. DOI: 10.1093/cybsec/tyab005
22. Thakur K, Ali ML, Jiang N et al. Impact of cyber-attacks on critical infrastructure. In: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016. New York, NY, USA.
23. CISA, Cyber Storm VI: National Cyber Exercise, D.o.H. Security, Editor, 2020. URL: http://www.cisa.gov/cyber-storm-vi
24. National cyber exercise: Cyber Storm VIII (CS VIII) States Working Group Overview Brief. Cyber Storm VIII July 2021. URL: http://www.tn.gov/content/dam/tn/cybersecurity/CS%20VIII%20States%20Brief.pdf (дата обращения: 18.01.2022).
25. Dorofeev, A.V., Markov, A.S. Conducting Cyber Exercises Based on the Information Security Threat Model // CEUR Workshop Proceedings, 2021, vol. 3057, pp. 1–10.
26. Дорофеев А.В., Марков А.С. Методические основы киберучений и CTF-соревнований // Защита информации. Инсайд. 2022. № 2 (104). С. 40—50.
27. Литвиненко А.В. Использование программных средств обеспечение безопасности Linux-сервера в рамках соревнований CTF // Вопросы кибербезопасности. 2013. № 3 (3). С. 33—35.
28. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3 (11). С. 2—14.

Рецензент: **Марков Алексей Сергеевич,** *доктор технических наук, старший научный сотрудник, профессор кафедры ИУ-7 МГТУ им. Н.Э. Баумана, г. Москва, Российская Федерация.*
E-mail: a.markov@bmstu.ru

CYBER EXERCISES: FOREIGN EXPERIENCE IN PROTECTING CRITICAL INFRASTRUCTURE

***Aleksandr Metel'kov*[2]**

Keywords: *cyber incidents, cyber threats, cyber security, modelling, information protection, information and communication technologies, coordination.*

Abstract.

Purpose of the work: identifying ways to improve the methods and means for ensuring information security based on the analysis of materials on cyber exercises carried out in the USA and other countries.

Method of study: multi-faceted theoretical and comparative analysis as well as generalisation of the experience obtained from research exercises carried out in the USA and other countries in cyberspace with a view to ensure corporate security. Using, in planning cyber exercises, simulations of training environment scenarios as an efficient method for a multi-faceted study of the system for response to cyber attacks and protection of public and private resources, systems and networks under the conditions of complexity and diversity of cyber attacks whose impact on the complex interdependent infrastructure of a number of sectors of modern human activity is quite difficult to describe using mathematical models. Studying foreign approaches shows the topicality of experimental methods for imitation simulation of cyber attacks on sensitive information infrastructure in various sectors of the economy and public administration.

Results obtained: the concept of cyber security is expounded and features of organisational and technical methods and means for ensuring it in the USA and other countries are highlighted. Foreign experience of simulating cyber attacks during large-scale cyber exercises is analysed, and it can be used in drills of cyber attack scenarios in domestic technologies of cyber training grounds for training specialists under the conditions of fast developing technologies and increasing cyber security risks. An imitation simulation model for a training scenario of realisation of cyber threats and a general model for cyber exercises organisational structure are proposed based on the generalisation of the experience.

References

1. Lallie H.S., Shepherd L.A., Nurse J.R.C., Erola A., Epiphaniou G., Maple C., Bellekens X. (2021). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security, 105, [102248]. URL: http://doi.org/10.1016/j.cose.2021.102248

[2] ***Aleksandr Metel'kov,*** *Ph.D. (Law), Associate Professor at the Department of Applied Mathematics and Information Technology of the Saint Petersburg University of the Russian State Fire Service of the Ministry of the Russian Federation for Civil Defence, Emergency Situations and Elimination of Consequences of Natural Disasters, Saint Petersburg, Russian Federation.*
E-mail: metelkov5178@mail.ru

2. Leblanc S.P., Partington A., Chapman I.M., Bernier M. An overview of cyber attack and computer network operations simulation. SpringSim (MMS), 2011, pp. 92–100.
3. Brown B., Cutts A., McGrath D., Nicol D.M., Smith T.P., Tofel B. Simulation of cyber-attacks with applications in homeland defense training. Sensors, and command, control, communications, and intelligence (c3i) technologies for homeland defense and law enforcement II. International Society for Optics and Photonics, 2003, Vol. 5071, pp. 63–71.
4. Kuhl M.E., Sudit M., Kistner J., Costantini K. Cyber-attack modeling and simulation for network security analysis. 2007 Winter Simulation Conference. IEEE, 2007, pp. 1180–1188.
5. Yamin M.M., Katt B., Gkioulos V. Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. Computers & Security 2019, p. 101636.
6. Radziwill N.M. Virginia cyber range. Software Quality Professional 2017, 19, 46.
7. Aliyu A, Maglaras L, He Y, Yevseyeva I, Boiten E, Cook A, Janicke H. A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. Applied Sciences. 2020; 10(10): 3660. URL: http://doi.org/10.3390/app10103660
8. Singh R, Kumar H, Singla R.K. et al. Internet attacks and intrusion detection system: a review of the literature. Online Inform Rev 2017; 41:171–84.
9. Bures M., Klima M., Rechtberger V., Bellekens X., Tachtatzis C., Atkinson R., Ahmed B.S. Interoperability and Integration Testing Methods for IoT Systems: A Systematic Mapping Study. Software Engineering and Formal Methods; de Boer, F.; Cerone, A., Eds.; Springer International Publishing: Cham, 2020; pp. 93–112.
10. Jason Kick. Cyber Exercise Playbook November 2014. URL: http://www.mitre.org/s/pr_14-3929-cyber-execise-playbook.pdf (data obrashcheniia: 18.01.2022).
11. Gore R, Padilla J, Diallo S. Markov chain modeling of cyber threats. J Def Model Simul 2017; 14:233–44.
12. Dobryshin M.M., Zakalkin P.V. Model' komp'iuternoi ataki tipa "phishing" na lokal'nuiu komp'iuternuiu set'. Voprosy kiberbezopasnosti, 2020, No. 2. C. 17–25.
13. Lavrova D.S., Zegzhda D.P., Zaitseva E.A. Modelirovanie setevoi infrastruktury slozhnykh ob"ektov dlia resheniia zadachi protivodeistviia kiberatakam. Voprosy kiberbezopasnosti, 2019, No. 2. S.13–20.
14. Miniaev A.A. Modelirovanie ugroz bezopasnosti informatsii v territorial'no-raspredelennykh informatsionnykh sistemakh. Naukoemkie tekhnologii v kosmicheskikh issledovaniiakh Zemli, 2021, t. 13, No. 2, pp. 52–65.
15. Japertas S, Baksys T. Method of early staged cyber-attacks detection in IT and telecommunication networks. Elektronika Ir Elektrotechnika, 2018; 24:68–77.
16. Selifanov V.V., Iurakova Ia.V., Karmanov I.N. Metodika avtomatizirovannogo vyiavleniia vzaimosviazei uiazvimostei i ugroz bezopasnosti informatsii v informatsionnykh sistemakh. Interekspo Geo-Sibir', 2018, No. 7, pp. 271–276.
17. Voronin V.V., Sukhorukov Ia.P. Aspekty razrabotki Chastnoi modeli ugroz bezopasnosti informatsii v tipovykh informatsionnykh sistemakh. Vestnik PGU im. Sholom-Aleikhema, 2020, No. 1, pp. 24–33.
18. Metodicheskii dokument "Metodika otsenki ugroz bezopasnosti informatsii", utv. FSTEK Rossii 5.02.2021. URL: http://fstec.ru
19. Vasil'ev V.I., Kirillova A.D., Vul'fin A.M. Kognitivnoe modelirovanie vektora kiberatak na osnove metashablonov CAPEC. Voprosy kiberbezopasnosti, 2021, No. 2, pp. 2–16.
20. Vasil'ev V.I., Vul'fin A.M., Kuchkarova N.V. Avtomatizatsiia analiza uiazvimostei programmnogo obespecheniia na osnove tekhnologii Text Mining. Voprosy kiberbezopasnosti, 2020, No. 4, pp. 22–31.
21. Kavak H., Padilla J.J., Vernon-Bido D., Diallo S.Y., Gore R.J., Shetty S. Simulation for Cybersecurity: State of the Art and Future Directions. Journal of Cybersecurity, Volume 7, Issue 1, 2021. DOI: 10.1093/cybsec/tyab005
22. Thakur K, Ali ML, Jiang N et al. Impact of cyber-attacks on critical infrastructure. In: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016. New York, NY, USA.
23. CISA, Cyber Storm VI: National Cyber Exercise, D.o.H. Security, Editor, 2020. URL: http://www.cisa.gov/cyber-storm-vi
24. National cyber exercise: Cyber Storm VIII (CS VIII) States Working Group Overview Brief. Cyber Storm VIII July 2021. URL: http://www.tn.gov/content/dam/tn/cybersecurity/CS%20VIII%20States%20Brief.pdf (data obrashcheniia: 18.01.2022).
25. Dorofeev, A.V., Markov, A.S. Conducting Cyber Exercises Based on the Information Security Threat Model. CEUR Workshop Proceedings, 2021, vol. 3057, pp. 1–10.
26. Dorofeev A.V., Markov A.S. Metodicheskie osnovy kiberuchenii i CTF-sorevnovanii. Zashchita informatsii. Insaid, 2022, No. 2 (104), pp. 40–50.
27. Litvinenko A.V. Ispol'zovanie programmnykh sredstv obespechenie bezopasnosti Linux-servera v ramkakh sorevnovanii CTF. Voprosy kiberbezopasnosti, 2013, No. 3 (3), pp. 33–35.
28. Petrenko A.A., Petrenko S.A. Kiberucheniia: metodicheskie rekomendatsii ENISA. Voprosy kiberbezopasnosti, 2015, No. 3 (11), pp. 2–14.