Научная статья
УДК 004.056; DOI: 10.61260/2218-13X-2025-2-91-101

МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ, СОБЫТИЙ И ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

✉**Метельков Александр Николаевич.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***metelkov5178@mail.ru***

Аннотация. Целью исследования является уточнение соотношения понятий компьютерных инцидентов, событий и инцидентов информационной безопасности. В научной литературе и стандартах появились разнообразные определения этих терминов, понимание которых усложняет практическую деятельность по реагированию на весь широкий и разнообразный спектр событий и инцидентов информационной безопасности. Для обнаружения признаков возможных угроз и их классификации с использованием нейросетей и машинного обучения необходимо более четкое представление о соотношении множеств компьютерных атак, событий и инцидентов информационной безопасности. В работе использованы методы сравнительного анализа документов, комплексный подход к изучению терминов и их содержания в сфере защиты информации. Поэтому сведение базовых понятий к единому пониманию будет способствовать совершенствованию системы реагирования. В результате исследования автором предложена модель взаимодействия вложенных множеств компьютерных атак, инцидентов и событий информационной безопасности, выделен перечень недопустимых событий.

Ключевые слова: событие, инцидент, угроза, компьютерная атака, реагирование, обнаружение, классификация

Для цитирования: Метельков А.Н. Модель взаимодействия компьютерных инцидентов, событий и инцидентов информационной безопасности // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 2. С. 91–101. DOI: 10.61260/2218-13X-2025-2-91-101.

Scientific article

MODEL OF INTERACTION BETWEEN COMPUTER INCIDENTS, EVENTS, AND INFORMATION SECURITY INCIDENTS

✉**Metel'kov Alexander N.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***metelkov5178@mail.ru***

Abstract. The purpose of the article is to clarify the relationship between the concepts of computer incidents, events and incidents of information security. Various definitions of these terms have appeared in the scientific literature and standards, the understanding of which complicates practical activities to respond to the entire wide and diverse range of information security events and incidents. To detect signs of possible threats and classify them using neural networks and machine learning, it is necessary to have a clearer understanding of the ratio of multiple computer attacks, events and incidents of information security. The paper uses methods of comparative analysis of documents, an integrated approach to the study of terms and their content in the field of information security. Therefore, reducing the basic concepts to a single understanding will help improve the response system. As a result of the research, the author proposed a model for the interaction of nested sets of computer attacks, incidents and information security events, the list of unacceptable events is highlighted.

Keywords: event, incident, threat, computer attack, response, detection, classification

For citation: Metel'kov A.N. Model of interaction between computer incidents, events, and information security incidents // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 2. P. 91–101. DOI: 10.61260/2218-13X-2025-2-91-101.

Введение

С начала 2022 г. тема управления инцидентами информационной безопасности (ИБ) как важнейшим процессом совершенствования системы управления ИБ становится наиболее значимой и актуальной для организаций и предприятий различных форм собственности, государства, общества и отдельных физических лиц. Развитие в этих условиях информационных технологий, совершенствование автоматизации управления, глобальная конструктивная роль сети Интернет, в то же время, влечет за собой опасность возрастания «эффективности и изощренности средств информационного воздействия, приводящих к огромным» последствиям [1, с. 40].

Нарушение политики ИБ, неавторизированный доступ, сбор информации, заражение вредоносным кодом, распространение информации с недопустимым содержанием представляют собой лишь некоторую часть событий, которые могут иметь отношение как к событиям и инцидентам ИБ, так и к компьютерным атакам.

Для любой организации государственного и частного сектора в современных условиях важно иметь надежную программу обеспечения ИБ, а также структурированный и спланированный подход к:

– планированию и подковке пользователей и персонала, обеспечивающего функционирование информационных систем (ИС), к управлению инцидентами ИБ, включая политику, организацию, план, техническую поддержку, повышение осведомленности, обучение навыкам и т.д.;

– обнаружению и анализу самых первых признаков ИБ для дифференциации реальных угроз от ложной тревоги;

– выявлению, сообщению и оценке инцидентов ИБ и уязвимостей, связанных с ними;

– реагированию на инциденты ИБ, включая активацию соответствующих средств контроля для предотвращения, уменьшения и восстановления ИС и сетей после воздействия;

– устранению выявленных уязвимостей ИБ, связанных с инцидентом;

– извлечению уроков из инцидентов ИБ и уязвимостей, связанных с ними;

– внедрению и проверке превентивных мер контроля и совершенствованию общего подхода к управлению инцидентами ИБ.

Системы обнаружения сетевых вторжений (IDS) и выявления признаков компьютерных атак в виде программных или аппаратно-программных решений широко используются в качестве технических средств защиты ИС. В поисках признаков угроз безопасности информации в IDS автоматизируется процесс контроля событий ИБ в информационной системе или компьютерной сети. Рост числа несанкционированных проникновений из различных источников в компьютерные сети и возрастание нагрузки на IDS, увеличение числа участков мониторинга стали условием формирования и наращивания базы данных, анализируемых подсистемами IDS. В процессе анализа осуществляется выявление отклонений параметров мониторинга, оцениваются показатели надежности выявления инцидентов ИБ. Увеличению показателей эффективности выявления таких инцидентов способствует уменьшение объема получаемых от подсистемы сбора информации данных, так как объективно увеличение объемов поступающей на вход исходной информации увеличивает время ее обработки и понижают эффективность работы системы. Достижению положительных результатов в решении задач распознавания образов вредоносного программного обеспечения (ПО), классификации и прогнозирования развития компьютерных атак помогает внедрение в процессы обработки первичной информации искусственных нейронных сетей (ИНС). Классификация информационных объектов является распространенной проблемой в искусственном интеллекте (ИИ), которую обычно решают

с помощью глубокого обучения ИНС, так как в процессе обучения они способны выявлять корреляции входных и выходных данных, которые отсутствовали в явном виде, для защиты компьютерной информации. Повышение эффективности выявления признаков и инцидентов ИБ в процессе мониторинга защищенности информационных ресурсов с использованием ИНС и совместно со статистическими методами анализа данных в единой системе является актуальной научно-технической задачей. IDS незаменимы для защиты конфиденциальной информации, хранящейся в сети. Методы машинного обучения (МО) все чаще используются при обеспечении кибербезопасности для защиты от компьютерных атак. Последствия кибератак смягчают с помощью статистических методов и методов МО. Применение МО позволяет значительно улучшить обнаружение вредоносных программ по сравнению с ручными операциями, а также повысить эффективность и уменьшить затраты. Интеллектуальные системы безопасности требуют обнаружения скрытых закономерностей и понимания сетевых данных с последующей разработкой модели МО на основе анализа данных для противодействия этим опасностям.

В работе [2] описывается использование ИИ при обнаружении, предотвращении и реагировании на CSRF- и XSS-атаки, кибератаки с использованием SQL-инъекций, что повышает возможности минимизации киберугроз в реальном времени. В исследовании [3, с. 115] зарубежными авторами обсуждаются ключевые компоненты для улучшения IDS с использованием ИНС, решения проблем и предоставления конкретных подходов улучшения путем внедрения новой модели ИНС для повышения устойчивости IDS к более распространённым состязательным атакам. Предлагаемая передовая технология обнаружения вторжений эффективно снижает риски и защищает цифровые системы от эскалации угроз кибербезопасности путем нейтрализации распространенных препятствий, таких как оптимизация гиперпараметров и работа с несбалансированными данными. Исследование демонстрирует эффективность усовершенствованных ИНС с точностью 92 % при решении более широких проблем в области ИИ, в частности, уязвимости нейронных сетей к вредоносным атакам. Для повышения безопасности будущие достижения сосредоточатся на использовании передовых алгоритмов глубокого обучения (DL), таких как сверточные нейронные сети.

События и инциденты: управление на основе признаков инцидентов ИБ и кибератак

Управление инцидентами ИБ в государственных органах представляет собой процесс обнаружения признаков и реагирования на связанные с ИС и данными инциденты. Содержанием этой деятельности является выявление подготовки и реализации угроз, предотвращение и минимизация возможного ущерба, восстановление ИС после инцидентов. В условиях роста числа кибератак, кибершпионажа, несанкционированного доступа к защищаемой информации, утечек сведений конфиденциального характера рассматриваемый «процесс выступает ключевым аспектом обеспечения информационной безопасности организации» [4, с. 41].

В основе обеспечения кибербезопасности новых цифровых систем находятся технологии анализа инцидентов безопасности и обнаружения кибератак. В свою очередь основой систем обнаружения и анализа являются методы сетевой безопасности (методы обнаружения на основе образов, граничных характеристик, прогнозной модели и методов обнаружения кибератак) и анализа коммуникаций, которые «значительно расширились за счет применения новых решений и искусственного интеллекта» [1, с. 159]. Для повышения эффективности процесса реагирования на инциденты (IR) в борьбе с неизвестными, сложными и изощренными киберугрозами, основные составляющие его действия (обнаружение, сдерживание, искоренение и восстановление) должны гибко реализовываться, что требует от групп IR наличия инструментов, навыков и умений анализировать признаки и данные о процессах, позволяющих собирать, интегрировать все сведения, выделять из них

критически важные для идентификации серьезной угрозы, связанной с инцидентами кибербезопасности, в масштабах всей территориально распределенной организации с целью своевременного принятия обоснованных решений и минимизации возможного ущерба.

Аналитика больших данных (BDA) используется в качестве организационной возможности собирать, интегрировать и анализировать большие объемы данных о процессах в организации, генерируемых с высокой скоростью в различных формах с целью получения информации для принятия обоснованных решений[5, 6].

В результате процесса управления уязвимостями организаций возможно обнаружение признаков компьютерных атак и вторжений в защищаемую информационную среду, а следовательно, выявление слабости в системе защиты информации. Противоречие между изменчивостью быстротечных компьютерных атак и инертностью механизмов их обнаружения становится критическим, что ослабляет «безопасность значимых объектов критической информационной инфраструктуры» [7, с. 3].

Быстро протекающий процесс осуществления угроз отличается этапами приготовления, маскировки компьютерных следов взлома, проникновения и выполнения деструктивных действий и «вероятностно-временными характеристиками» их реализации [8, с. 10]. В этом процессе ключевым является проникновение в операционную среду и осуществление несанкционированного воздействия.

Обнаружение инцидентов ИБ сводится к задаче классификации. В работе [9] выделяют методы обнаружения атак на ИС с использованием экспертных систем, анализа систем состояний, графов сценариев атак, сигнатурных методов, нейронных и иммунных сетей, статистического и кластерного анализа, поведенческой биометрии и др.

В целях обнаружения и расследования инцидентов в информационной инфраструктуре, кроме выявления потенциально небезопасных событий, необходимо отбирать и связанные друг с другом события. Разработанный математический метод анализа инцидентов ИБ с использованием корреляции событий содержит корреляцию двух событий безопасности, а также событий безопасности текущих событий [10, с. 266]. Принимая во внимание сложность данного метода анализа инцидентов ИБ, все множество событий *Event*=$\{event_1$,$event_2$, … $event_n\}$ разделяется на класс обычных событий и класс априорно небезопасных и потенциально небезопасных событий.

Класс обычных событий: $Event^{Normal}$ Event = $\{ event\,_1^{Normal}$,$event\,_2^{Normal}$, $event\,_K^{Normal}\}$, *event Normal Apriory Insecure Event Poten.* Класс событий безопасности $Event^{Insecure}$, подразделяемый на подкласс априорно небезопасных событий: $Event^{Apriory\ Insecure}=\{event_1^{Apriory\ Insecure}$, $event_2^{Apriory\ Insecure}$, … $event_N^{Apriory\ Insecure}\}$, и подкласс потенциально небезопасных событий: $Event^{Poten\ Insecure}=\{event_1^{Poten\ Insecure}$, $event_2^{Poten\ Insecure}$, … $event_N^{Poten\ Insecure}\}$.

При анализе событий ИБ построение цепочек событий начинается с заведомо небезопасного.

Для обнаружения компьютерных атак в критической информационной инфраструктуре представлена система управления, «реализующая выбор детекторов атак в режиме реального времени, за счет комбинирования нейросетей и аппарата нечеткой логики» [7, с. 10]. Широкое применение для решения задачи обнаружения сетевых атак получили методы ИИ, такие как нейросети и алгоритмы МО [11, 12].

В основе теории организации реагирования на угрозы ИБ лежит научная терминология, например, такие термины как «событие ИБ», «инцидент ИБ», «компьютерная атака» и др. В литературе и стандартах нет четкого определения каждого из этих терминов, что затрудняет понимание их взаимосвязи. Полисемия в содержании терминов затрудняет построение моделей, в которых используется понятие «инциденты ИБ».

Сравнительный анализ определений в таблице показывает, что в одних инцидент ИБ рассматривается как единичное событие, в других – как одно или несколько (серия) событий,

в-третьих – как любое событие. События носят неожиданный, непредвиденный или нежелательный характер. В определениях и их содержание раскрывается по-разному через:

– угрозу нарушения деятельности или ИБ;

– значительную вероятность компрометации бизнес-операции и угрозу ИБ;

– возможность нарушения деятельности или ИБ;

– значительную вероятность компрометации бизнес-операций и создания угрозы ИБ (то есть угрозы пока ещё нет, но она с определенной вероятностью может появиться).

Таблица

Сравнительно-правовой анализ целей защиты информации

Наименование документа	Определение понятия «инцидент ИБ»
ГОСТ Р 59709–2022, ГОСТ Р53114–2008, ISO 27000, NIST800–61	Непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (могут привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации, нарушению требований по защите информации
ГОСТ Р ИСО/МЭК ТО 18044–2007	Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ
ГОСТ Р 54147–2010	Одно или серия нежелательных или неожиданных событий ИБ, которые имеют значительную вероятность компрометации бизнес-операции и угрожают ИБ
ГОСТ Р ИСО/МЭК 27001–2006	Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или ИБ

Составители Рекомендаций в области стандартизации Банка России РС БР ИББС-2.5-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности» под инцидентом понимают событие или их комбинацию, указывающую на реализацию угрозы ИБ, итогом которой может стать:

– нарушение в системе обеспечения ИБ и работе средств защиты информации;

– нарушение требований законодательства, нормативных правовых актов и предписаний регулирующих и надзорных органов, локальных документов организации по обеспечению ИБ;

– нарушение выполнения процессов системы менеджмента ИБ и «технологических процессов организации;

– нанесение ущерба как организации, так и ее клиентам» [13].

В Руководстве по обработке инцидентов компьютерной безопасности Национального института стандартов и технологий США под событием понимается любое наблюдаемое в системе или сети событие, не вызванное стихийными бедствиями и не связанное со сбоями электропитания и т.д. События включают в себя подключение пользователя к сервису обмена файлами, блокировку межсетевым экраном попытки подключения и т.п. К неблагоприятным событиям относят события с негативными последствиями. Инцидент компьютерной безопасности рассматривается как нарушение или неминуемая угроза нарушения политик компьютерной безопасности, политик допустимого использования или стандартных методов безопасности. Такими инцидентами являются следующие:

– злоумышленник дает команду ботнету направить множество запросов на подключение к веб-серверу, что приводит к его сбою;

– обманом заставляют пользователей открыть документ, отправленный по электронной почте, который является вредоносным ПО, после чего запускается инструмент для заражения компьютеров пользователей и установления соединения с внешним хостом;

– вымогатель добывает конфиденциальные данные и угрожает их опубликованием в случае неуплаты организацией-жертвой указанного злоумышленникам «выкупа»;

– пользователь распространяет сведения конфиденциального характера другим лицам через одноранговые службы обмена файлами [14].

Атаки часто ставят под угрозу государственные информационные ресурсы, деловые и персональные данные, поэтому необходимо своевременно реагировать на инциденты ИБ. Это помогает персоналу минимизировать ущерб, последствия сбоев в функционировании информационной инфраструктуры, совершенствовать меры защиты информации. Для своевременного реагирования на инциденты и их обработку необходимо внедрять систему оповещения об инцидентах.

Инциденты ИБ классифицируют на компьютерные, технические, организационные и технологические. Компьютерные инциденты ИБ связаны с обработкой информации в автоматизированных системах, технические предполагают выход/вывод из строя аппаратных средств, организационные вызваны деятельностью персонала, технологические обусловлены нарушением «работоспособности технологических элементов и т.п.» [15, с. 55].

Примерами компьютерных инцидентов являются «отказ в обслуживании системы; заражение вирусами; несанкционированный доступ к информации и т.д.» [16, с. 55], а инцидентов ИБ – ошибки пользователей; нарушение правил доступа; несоблюдение политики или рекомендаций по ИБ; нарушение мер физзащиты; сбои ПО и отказы технических средств; системные сбои или перегрузки; утрата услуг, оборудования или устройств и др.

В учебной литературе используется термин «типовая удаленная атака», то есть «удаленное информационное воздействие, осуществляемое с помощью программ по каналам связи и характерное для любой распределенной информационной системы» [15, с. 183]. Если в работе компьютера обнаружен хотя бы один признак, то с большой долей вероятности можно предположить, что компьютер заражен вредоносной программой [15, с. 223].

Среди видов кибератак выделяют анализ сетевого трафика, сканирование сети, подмену доверенного объекта сети, ложный объект сети, отказ в обслуживании (Dos-, DDoS-атаки), подбор пароля [15, с. 183].

Для защиты от угроз несанкционированного доступа и компьютерных атак в автоматизированных системах применяют средства разграничения доступа, обеспечения целостности информации, антивирусной защиты, анализа защищенности, «криптографические средства, средства, системы обнаружения вторжений, системы предотвращения вторжений, межсетевые экраны» и др. [17, с. 48].

Поэтому автором предлагается следующая модель их взаимодействия с использованием теории множеств: A – множество компьютерных атак, B – множество инцидентов ИБ, C – множество событий ИБ (рис. 1). Формализованная запись с помощью математического аппарата теории множеств будет выглядеть как $A \subset B \subset C$.

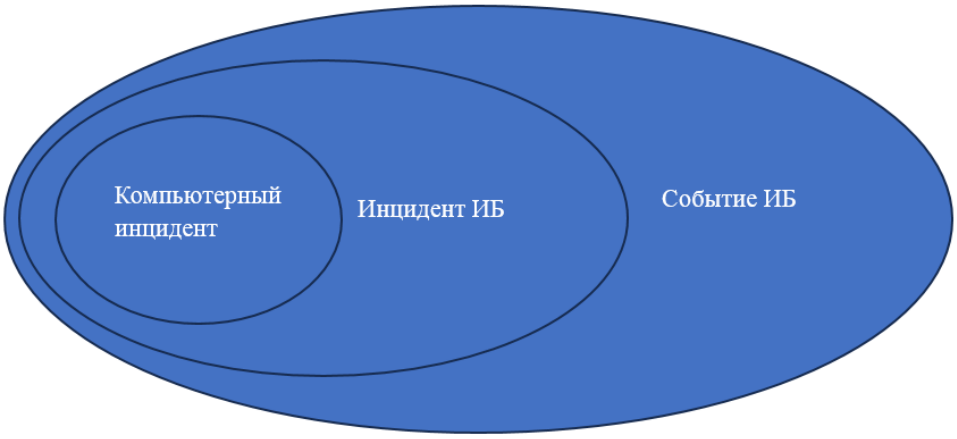

Рис.1. **Модель взаимодействия компьютерных атак, событий и инцидентов ИБ**

Исходя из определения события ИБ как «состояния», а инцидента ИБ как «события», сложно построить модель их взаимодействия. Поэтому автор предлагает трактовать понятие «событие ИБ» как появление признака или их совокупности, характеризующих возникновение состояния системы, услуги или сети, и указывающего (-их) на возможное нарушение политики ИБ, аварию защитных средств, нарушение правил, а также возникновение ранее неизвестной ситуации, возможно связанной с безопасностью. Это позволит рассматривать множество событий ИБ как множество признаков ИБ. Например, признаки, которые могут свидетельствовать о заражении компьютера, показаны на рис. 2.

Рис. 2. **Признаки заражения компьютера**

Компьютерная атака в стандартах определена как «целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и (или) создания угрозы безопасности обрабатываемой таким ресурсом информации» [18], «несанкционированное воздействие на информацию, на ресурс автоматизированной ИС или получение несанкционированного доступа к ним» [19].

В случае пропуска начала атаки злоумышленнику удается проникнуть внутрь сетевой инфраструктуры «незамеченным или легитимные с точки зрения работы системы действия могут повлечь за собой атаку» [8, с. 266].

Управление инцидентами ИБ в организации – это процесс идентификации, анализа и реагирования на инциденты, связанные с ИС и данными. Управление инцидентами включает комплекс мероприятий по предотвращению, минимизации ущерба и восстановлению

нормального функционирования систем. Организации подвергаются кибератакам, несанкционированному доступу к их информации, утечкам сведений конфиденциального характера, физическому разрушению элементов ИС, влекущим «финансовые потери и подрыв репутации компании» [4, с. 41].

Управление инцидентами ИБ в государственных, муниципальных и иных ИС представляет собой элемент стратегии безопасности, обеспечивает ответную реакцию на угрозы, формирует проактивный подход к предотвращению инцидентов ИБ.

Чтобы обезопасить компьютерную систему от злоумышленников, отдельные лица, организации, разработчики ПО и страны должны сотрудничать для обеспечения всесторонней защиты. В этом контексте решения можно разделить на технические и нетехнические. При работе с кибератаками административное управление, политики, стандарты, процедуры, оценка рисков, управление поставщиками, распределение обязанностей и обучение являются критически важными нетехническими концепциями. Даже если специалисты по кибербезопасности создадут самую хорошо спроектированную систему защиты, адекватная безопасность не будет обеспечена без должного обучения пользователей.

Создание интеллектуальных приложений при борьбе с умышленными угрозами предусматривает технические решения, в которых реализуются технологии искусственного интеллекта, обработки и анализа большого объема данных (big data), машинного обучения и когнитивные технологии, криптографические методы защиты информации. В частности, криптография защищает целостность и конфиденциальность данных. Повышению уровня их безопасности способствует метод контроля доступа. Большие данные позволяют анализировать значительный объем информации для обнаружения неизвестных шаблонов, а также вредоносных функций атак. Методы виртуализации отделяют программные приложения от аппаратных компонентов, что повышает удобство использования ПО и снижает стоимость, одновременно сокращая время простоя в случае кибератак. Платформа облачных вычислений обеспечивает упреждающее управление угрозами, расширенную безопасность данных, их масштабируемость, высокую доступность и эффективное восстановление. Технология блокчейн помогает проверять согласованность данных, а также обнаруживать некоторые сложные атаки. Статистические методы позволяют интерпретировать и выявлять шаблоны в данных. Интеллектуальный анализ данных обнаруживает и извлекает неизвестные шаблоны в больших наборах данных. Методы МО помогают добавлять новые функции в существующие системы обнаружения атак. Инновационные технологии МО повысили эффективность систем обнаружения последних разновидностей кибератак.

Однако, технические достижения, значительно улучшающие способность сканирования на предмет утечек данных, нахождения уязвимостей в компьютерных системах и сетях связи и повышения точности систем обнаружения атак, не решают весь набор проблем, связанных с эффективным обнаружением новых и постоянно усложняющихся кибератак. Эти проблемы заключаются в том, что атаки становятся автоматизированными с помощью кибератак как услуга; интеллектуальные атаки обходят системы обнаружения; алгоритмы на основе МО делают предположения о данных, которые содержат предвзятость; классификация миллионов сетевых соединений является сложной задачей; работа с данными высокой размерности обременительна; защита нескольких компонентов является надежной; безопасность часто превращается в проблему человеческого фактора [20].

Важные для реагирования на наиболее опасные инциденты ИБ, способные привести к недопустимым событиям, к которым, на взгляд автора, могут быть отнесены следующие события: разглашение персональных данных, финансовый или иной материальный ущерб

физическому лицу, ущерб здоровью человека (ущерб физическому лицу); нарушение законодательства Российской Федерации в части обеспечения безопасности информации, экономический ущерб в форме штрафов, материальный ущерб юридическому лицу, репутационный ущерб, выход из строя технических средств и программного обеспечения (ущерб оператору); событие влекущее нарушение выполнения органом власти возложенных на него функций, нарушения предоставления государственных услуг(ущерб в социальной сфере) и др. Перечень таких недопустимых событий оператор ИС должен устанавливать с учетом обстановки и условий, в которых функционирует та или иная ИС.

Выводы

Сбор информации о признаках проявления компьютерных атак среди большого множества событий и инцидентов ИБ, накопление и постоянное наращивание информации о таких признаках с учетом средств защиты и уязвимостей ИС позволит обеспечивать адекватное реагирование на современные угрозы и применять более совершенные методы анализа сведений о событиях и инцидентах ИБ с учетом их возможных связей и зависимостей.

Один или несколько признаков, с высокой степенью вероятности определяющих угрозы безопасности информации, должны учитываться при алгоритмизации процессов обнаружения киберугроз и МО на основе постоянно накапливаемых больших данных о признаках инцидентов ИБ.

Статья подготовлена в рамках выполнения в 2025 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России НИР «Исследование способов мониторинга и реагирования на возможные инциденты информационной безопасности в цифровой информационной инфраструктуре МЧС России и разработка организационно-технических предложений по их реализации» (НИР «Кибермониторинг»).

Список источников

1. Зегжда Д.П. Теоретические основы киберустойчивости и практика прогностической защиты от кибератак: монография. СПб.: ПОЛИТЕХ-ПРЕСС, 2022. 490 с.

2. Вильховский Д.Э. Возможности ИИ в сфере кибербезопасности: вопросы обнаружения, предотвращения и реагирования на SQL-инъекции, XSS- и CSRF-атаки // Математические структуры и моделирование. 2024. №4. С. 111–124.

3. Oyinloye T.S., Arowolo M.O., Prasad R. Enhancing cyber threat detection with an improved artificial neural network model // Data Science and Management. 2025. № 8. P. 107–115.

4. Моделирование процессов управления инцидентами информационной безопасности на предприятии / Е.С. Митяков [и др.] // Russian Technological Journal. 2024. Т. 12. № 6. С. 39−47.

5. Muller O., Junglas I., Brocke J. The use of Big Data analytics for Information Systems research: Problems, Promises and Recommendations // European Journal of Information Systems. 2016. № 25 (1). P. 289–202.

6. Mikalef P., Krogsti J. Exploring the interaction between big data analytics and contextual factors in stimulating process innovation opportunities // European Journal of Information Systems. 2020. № 29 (3). P. 260–287.

7. Крундышев В.М. Автоматизированная система анализа киберугроз в критической информационной инфраструктуре: автореф. дис. … канд. техн. наук. Санкт-Петербург, 2021. 19 с.

8. Язов Ю.К. Основы теории составных сетей Петри-Маркова и их применения для моделирования процессов реализации угроз безопасности информации в информационных системах: монография. СПб.: Сциентиа, 2024. 196 с.

9. Исследование нейросетевых технологий для выявления инцидентов информационной безопасности / Р.А. Марков [и др.] // Молодой ученый. 2015. № 23 (103). С. 55–60.

10. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / под ред. Д.П. Зегжда. М.: Горячая линия-Телеком, 2023. 560 с.

11. Павленко Е.Ю. Выявление вредоносных Android-приложений с использованием сверточной нейронной сети // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 107–119.

12. Зегжда П.Д. Использование искусственной нейронной сети для определения автоматически управляемых аккаунтов в социальных сетях // Проблемы информационной безопасности. Компьютерные системы. 2016. № 4. С. 9–15.

13. Майорова Е.В. Методические аспекты реагирования на инциденты информационной безопасности в условиях цифровой экономики // Петербургский экономический журнал. 2020. № 1. С.158–159.

14. Computer Security Incident Handling Guide. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (дата обращения 13.02.2025).

15. Бабаш А.В. Угрозы и риски информационной безопасности субъекта экономической деятельности: учеб. пособие. М.: ФГБОУ ВО «РЭУ им. Г.В. Плеханова», 2022.144 с.

16. Сычев Ю.Н. основы информационной безопасности: учеб. пособие. М.: ИНФРА-М, 2023. 337 с.

17. Авраменко В.С., Маликов А.В., Селезнев А.В. Проблемы управления событиями и инцидентами информационной безопасности в автоматизированных системах специального назначения // Техника средств связи. 2018. № 2 (142). С.48–52.

18. ГОСТ Р 59709–2022 Защита информации. Управление компьютерными инцидентами. Термины и определения. Издание официальное. М.: Российский институт стандартизации, 2022. 16 с.

19. ГОСТ Р 56939–2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования. Издание официальное. М.: Стандартинформ, 2016. 24 с.

20. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions / Ö. Aslan [et al.] // Electronics. 2023. Vol. 12. № 6. P. 1333. https://doi.org/10.3390/electronics12061333.

References

1. Zegzhda D.P. Teoreticheskie osnovy kiberustojchivosti i praktika prognosticheskoj zashchity ot kiberatak: monografiya. SPb.: POLITEH-PRESS, 2022. 490 s.

2. Vil'hovskij D.E. Vozmozhnosti II v sfere kiberbezopasnosti: voprosy obnaruzheniya, predotvrashcheniya i reagirovaniya na SQL-in"ekcii, XSS- i CSRF-ataki // Matematicheskie struktury i modelirovanie. 2024. №4. S. 111–124.

3. Oyinloye T.S., Arowolo M.O., Prasad R. Enhancing cyber threat detection with an improved artificial neural network model // Data Science and Management. 2025. № 8. P. 107–115.

4. Modelirovanie processov upravleniya incidentami informacionnoj bezopasnosti na predpriyatii / E.S. Mityakov [i dr.] // Russian Technological Journal. 2024. T. 12. № 6. S. 39−47.

5. Muller O., Junglas I., Brocke J. The use of Big Data analytics for Information Systems research: Problems, Promises and Recommendations // European Journal of Information Systems. 2016. № 25 (1). P. 289–202.

6. Mikalef P., Krogsti J. Exploring the interaction between big data analytics and contextual factors in stimulating process innovation opportunities // European Journal of Information Systems. 2020. № 29 (3). P. 260–287.

7. Krundyshev V.M. Avtomatizirovannaya sistema analiza kiberugroz v kriticheskoj informacionnoj infrastrukture: avtoref. dis. … kand. tekhn. nauk. Sankt-Peterburg, 2021. 19 s.

8. Yazov Yu.K. Osnovy teorii sostavnyh setej Petri-Markova i ih primeneniya dlya modelirovaniya processov realizacii ugroz bezopasnosti informacii v informacionnyh sistemah: monografiya. SPb.: Scientia, 2024. 196 s.

9. Issledovanie nejrosetevyh tekhnologij dlya vyyavleniya incidentov informacionnoj bezopasnosti / R. A. Markov [i dr.] // Molodoj uchenyj. 2015. № 23 (103). S. 55–60.

10. Kiberbezopasnost' cifrovoj industrii. Teoriya i praktika funkcional'noj ustojchivosti k kiberatakam / pod red. D.P. Zegzhda. M.: Goryachaya liniya-Telekom, 2023. 560 s.

11. Pavlenko E.Yu. Vyyavlenie vredonosnyh Android-prilozhenij s ispol'zovaniem svertochnoj nejronnoj seti // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy. 2018. № 3. S. 107–119.

12. Zegzhda P.D. Ispol'zovanie iskusstvennoj nejronnoj seti dlya opredeleniya avtomaticheski upravlyaemyh akkauntov v social'nyh setyah // Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy. 2016. № 4. S. 9–15.

13. Majorova E.V. Metodicheskie aspekty reagirovaniya na incidenty informacionnoj bezopasnosti v usloviyah cifrovoj ekonomiki // Peterburgskij ekonomicheskij zhurnal. 2020. № 1. C.158–159.

14. Computer Security Incident Handling Guide. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (data obrashcheniya 13.02.2025).

15. Babash A.V. Ugrozy i riski informacionnoj bezopasnosti sub"ekta ekonomicheskoj deyatel'nosti: ucheb. posobie. M.: FGBOU VO «REU im. G.V. Plekhanova», 2022.144 s.

16. Sychev Yu.N. osnovy informacionnoj bezopasnosti: ucheb. posobie. M.: INFRA-M, 2023. 337 s.

17. Avramenko V.S., Malikov A.V., Seleznev A.V. Problemy upravleniya sobytiyami i incidentami informacionnoj bezopasnosti v avtomatizirovannyh sistemah special'nogo naznacheniya // Tekhnika sredstv svyazi. 2018. № 2 (142). S.48–52.

18. GOST R 59709–2022 Zashchita informacii. Upravlenie komp'yuternymi incidentami. Terminy i opredeleniya. Izdanie oficial'noe. M.: Rossijskij institut standartizacii, 2022. 16 s.

19. GOST R 56939–2016 Zashchita informacii. Razrabotka bezopasnogo programmnogo obespecheniya. Obshchie trebovaniya. Izdanie oficial'noe. M.: Standartinform, 2016. 24 s.

20. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions / Ö. Aslan [et al.] // Electronics. 2023. Vol. 12. № 6. P. 1333. https://doi.org/10.3390/electronics12061333.

Информация о статье:
Статья поступила в редакцию: 11.02.2025; одобрена после рецензирования: 22.04.2025;
принята к публикации: 26.04.2025
Information about the article:
The article was submitted to the editorial office: 11.02.2025; approved after review: 22.04.2025;
accepted for publication: 26.04.2025

Сведения об авторах:
Метельков Александр Николаевич, доцент кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат юридических наук, e-mail: metelkov5178@mail.ru, https://orcid.org/0000-0002-6113-8981, SPIN-код: 5990-6833

Information about the authors:
Metel'kov Alexander N., associate professor of the department of applied mathematics and information technology security Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of law, e-mail: metelkov5178@mail.ru, https: //orcid.org/0000-0002-6113-8981, SPIN: 5990-6833