ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ СИСТЕМ УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Ганиев Салим Каримович, доктор технических наук, профессор, ТУИТ.
Султонов Йулдошбой Оразметбоевич, магистрант, ТУИТ.

Аннотация. В данной статье, на основе анализа научных источников, международных и отечественных стандартов и рекомендаций, сделана попытка систематизации принципов и формализации процедур разработки систем управления инцидентами информационной безопасности. Также, на базе частных обобщений, определены фазы жизненного цикла инцидентов и приведены компоненты типовой системы управления инцидентами информационной безопасности. Кроме того, показаны номенклатуры европейских групп реагирования на инциденты информационной безопасности CERT / CSIRT.

Ключевые слова: инцидент информационной безопасности, управления инцидентами, группа реагирования на инциденты информационной безопасности, система управления инцидентами информационной безопасности.

Управление инцидентами является одной из важнейших процедур управления информационной безопасностью (ИБ). В библиотеке лучших ИТ-практик ITIL под понятием «инцидент» понимается любое событие, не являющееся элементом нормального функционирования определенного сервиса и при этом влияет, или способна повлиять на работу этого сервиса путем его прерывания или снижения качества. В соответствии с действующими международных и отечественных стандартов в области управления инцидентами информационной безопасности (УИИБ) [1, 2], первым и важнейшим шагом является своевременное и корректное устранения последствий инцидента. Далее, необходимо расследовать инцидент, выполнить оценку необходимости действий по устранению причин инцидента, если нужно - реализовать их, а также выполнить действия по предупреждению повторного возникновения инцидента (превентивные меры). Кроме этого, важно сохранять все данные об инцидентах ИБ, ведь с помощью статистики инцидентов можно определить наиболее актуальные угрозы для организации и, соответственно, максимально точно планировать мероприятия по повышению уровня защищенности информационно-коммуникационных систем (ИУС) организации. Именно этот факт, по нашему мнению, и определяет актуальность построения и исследования эффективности работы систем управления инцидентами информационной безопасности (СУИИБ).

Целью исследования является освещение основных процедур и процессов, связанных с организацией и сопровождением систем менеджмента инцидентов информационной безопасности.

Согласно [3] УИИБ - это процесс или набор процессов, на вход которых подаются данные, полученные в результате сбора и протоколирования данных о событиях, касающихся ИКС, а на выходе этих процессов получают информацию о причинах инцидента, произошедшего, об ущербе, нанесен организации, и мерах, которые необходимо принять для того, чтобы инцидент не повторился. Таким образом, УИИБ направлен на совершенствование системы обеспечения безопасности организации. Кроме того, выходные данные есть, по сути, единственным объективным параметром в определении вероятности реализации угроз при анализе рисков. Эффективность процесса УИИБ зависит от: координации и согласованности действий всех вовлеченных в него лиц; имеющихся возможностей по получению и анализу информации, связанной с инцидентом; оперативности и корректности полученных результатов. Повышение каждого из приведенных показателей заметно повысит эффективность всего процесса и, тем самым, позволит подразделения ИБ организации приобрести более значительных результатов. Используя СУИИБ можно радикально изменить ситуацию эффективности управления инцидентами. Таким образом, СУИИБ фактически будет системой коллективной работы, которая автоматизирует процессы с УИИБ с помощью интеграции людей и аппаратно-программного обеспечения мониторинга и защиты, а также информационной инфраструктуры организации.

Предположение о том, что в организации произошел инцидент ИБ, должна базироваться на трех основных факторах [3]: 1) Сообщение об инциденте ИБ поступают одновременно из нескольких источников (пользователи, IDS, файлы журналов и т.д.); 2) IDS сигнализируют о многократное повторение определенных событий; 3) Анализ файлов журналов автоматизированной системы (АС) дает основание для вывода о возможности наступления инцидента.

В общем случае, признаки инцидента делятся на две основные категории - сообщение о том, что инцидент происходит в данный момент и сообщение о том, что инцидент, возможно, состоится в будущем.

Принятие решения о наступлении инцидента во многом зависит от компетентности экспертов команды реагирования. Они должны четко отличать случайную ошибку оператора, например, от вредоносных целенаправленного воздействия на ИКС. В документах [4, 5] приведены основные принципы организации и функционирования команд (групп) реагирования на инциденты ИБ CERT / CSIRT, а документ [6] содержит перечень и месторасположение действующих команд CERT / CSIRT по данным Европейского агентства по вопросам сетей и ИБ.

Как показал проведенный анализ [1, 2], сегодня в международной практике разработаны достаточное количество нормативных документов различного характера (стандарты, рекомендованные практики, руководства и т.п.), регламентирующих вопросы УИИБ. Согласно [3] для эффективного УИИБ необходимо организовать комплекс процессов управления инцидентами, обеспечить его надлежащими ресурсами, соответствующей нормативно-распорядительной и рабочей документацией, техническими средствами обеспечения механизмов контроля. Для обработки событий и инцидентов ИБ необходимо организовать процесс реагирования на инциденты. Затем следует разработать необходимые нормативные документы по управлению инцидентами. Как правило, такие документы должны описывать: 1) Определение инцидента ИБ - перечень событий, является инцидентами (то есть, именно в этой организации является инцидентом ИБ); 2) Порядок оповещения ответственного лица о возникновении инцидента (необходимо определить формат отчета, а также отразить контактную информацию лиц, которые должны оповещать об инциденте) 3) Порядок устранения последствий и причин инцидента; 4) Порядок расследования инцидента (определение причин инцидента, виновных в возникновении инцидента, порядок сбора и хранения доказательств); 5) Внесение дисциплинарных взысканий; 6) Реализация корректирующих и превентивных мер.

В рамках СУИИБ необходимо собирать и обрабатывать большое количество событий ИБ, которые поступают из разных источников. Эти события должны быть приведены к единому виду, что позволяет применять единые алгоритмы обработки и безошибочного выделения из них именно инцидентов ИБ. Необходимо сохранять события ИБ в течение времени, достаточного для обеспечения расследования инцидентов. Нужно разработать архитектуру СУИИБ, спроектировать комплекс решений, реализующих данную архитектуру, выбрать комплекс технических средств, осуществить внедрение системы. При разработке технических решений необходимо учитывать особенности функционирования инфраструктуры информационных технологий (ИТ-инфраструктуры) организации, имеющиеся средства автоматизации и тому подобное. Для эффективного функционирования СУИИБ необходимо, на стадии внедрения, обеспечить ряд ключевых факторов. В первую очередь, система управления должна быть обеспечена входным потоком событий ИБ, адекватно отражает состояние в рамках выбранной области действия. При обнаружении и реагировании на инцидент, необходимо иметь данные о задействованных ресурсов (активов), их владельцев и степень критичности, а также иметь доступ к данным о событиях, повлиявших на инцидент ИБ, таких как данные аудита действий пользователей и администраторов. При предоставлении отчетности об инцидентах руководству, необходимо иметь возможность сопоставления ресурсов,

подвергшихся влиянию в результате инцидента и рисков для основных бизнес-процессов организации.

Согласно [3] работы по внедрению СУИИБ предлагается проводить в несколько этапов: обследование объекта; разработка процедур и процессов системы управления, написание соответствующих документов; внедрение СУИИБ; внедрение АС мониторинга и управления инцидентами ИБ. Для визуализации результатов анализа событий, происходящих в информационной системе, используется составления диагностических матриц. Матрица формируется из строк потенциальных признаков инцидента и столбцов - типов инцидентов. Дается оценка события по шкале приоритетов - «высокий», «средний», «низкий». Диагностическая матрица призвана документировать ход логических выводов экспертов в процессе принятия решения и, наряду с другими документами, служит свидетельством расследование инцидента. При анализе инцидентов ИБ организация должна выполнить следующие действия: своевременно идентифицировать неудачные и успешные нарушения и инциденты ИБ; помочь в выявлении событий безопасности, таким образом предотвратить инциденты безопасности путем использования индикаторов. Управление инцидентами ИБ должно включать следующие действия: сообщение о уязвимые места ИКС и события ИБ; ответственность и процедуры; обучение на инцидентах ИБ; сбор доказательств. Документирования событий инцидента ИБ необходимо, прежде всего, для сбора и консолидации технологических и операционных свидетельств расследования. Документированию подлежат все факты и доказательства злонамеренного воздействия, типичной практикой является ведение журнала расследование инцидента, который не имеет стандартной формы и разрабатывается командой CERT / CSIRT.

Архитектура типичной СУИИБ должна включать следующие основные компоненты [3]: интеграционную платформу; аппаратно-программные средства мониторинга и аудита; аппаратно-программные средства защиты информации; хранилище информации об инцидентах ИБ; аналитические инструменты и средства генерации отчетов средства управления и пользовательские интерфейсы. Интеграционная платформа является ядром системы, она призвана обеспечивать четкую и оперативную координацию и взаимодействие лиц, отвечающих за реакцию на события, связанные с инцидентами ИБ. Аппаратно-программные средства мониторинга и аудита - средства, реализующие функции по протоколированию, сбора, накопления и обработки информации о функционировании ИКС организации. Они составляют подсистему сбора информации об инцидентах ИБ. Результатом их работы сведения, на основе которых системой принимается решение о наступлении инцидента. Аппаратно-программные средства защиты в контексте СУИИБ -это средства, обеспечивающие локализацию инцидентов или снижение ущерба. Эти средства имеют механизмы, позволяющие проводить

быструю и дистанционное изменение своей конфигурации или иметь в своем составе заранее разработанные автоматизированные сценарии действий по минимизации возможного ущерба от инцидентов ИБ. Также, в организации должна быть разработана и внедрена система оповещения об инцидентах.

Обобщенной целью обеспечения ИБ организации является снижение рисков, действующих в отношении информационных ресурсов, и как следствие предотвращения или минимизации ущерба от возможных инцидентов ИБ. Основной задачей процесса УИИБ является устранение инцидентов в предельно сжатые сроки. В ходе процесса управления инцидентами ИБ проводится выявление, регистрация, классификация и начальная поддержка запросов, а также поиск решения, его применение, контроль, информирование и подготовка отчетности. Поскольку, как мы уже определили, инцидентом, в первую очередь, есть определенная непозволительная событие, то она должна быть кем-то запрещена. Следовательно, существует необходимость разработки и утверждения документов, четко описывают все действия, которые можно выполнять в ИКС и которые выполнять запрещено.

Одной из лучших СУИИБ среди присутствующих на отечественном рынке является программный продукт для обработки событий - netForensics nFX Open Security Platform [3], показан на рис. 1:

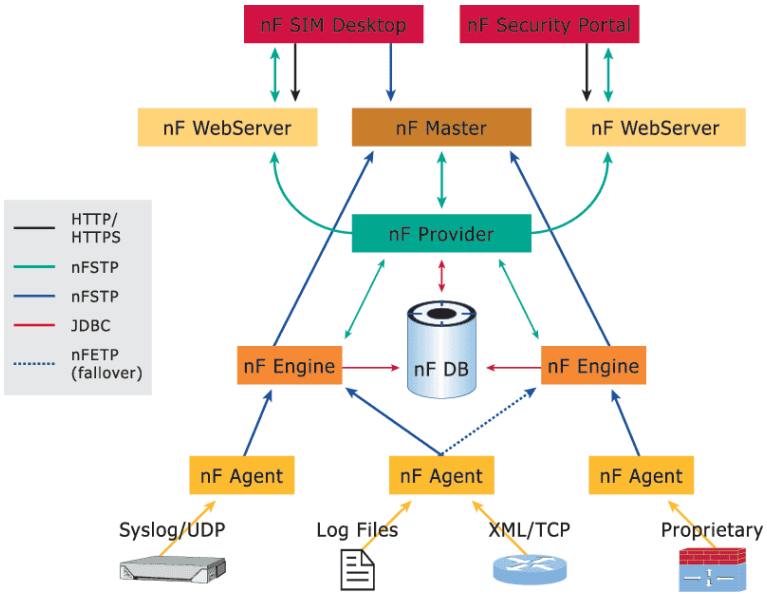

Рис. 1. СУИИБ netForensics

Система netForensics предназначена для работы с гетерогенной средой продуктов обеспечения ИБ и реализует непрерывный сбор, обработку и отображение событий безопасности. Система может работать на платформах Windows, Linux или Solaris, используя в качестве хранилища данных полнофункциональную СУБД Oracle. Эта СУИИБ имеет широкие возможности работы в распределенной режиме, поддержку различных отказоустойчивых конфигураций и тому подобное. СУИИБ netForensics реализована на базе технологии Java по модульному

принципу. Основными модулями системы является сервер приложений (реализует основную логику обработки событий, представления данных, взаимодействия с пользователями) база данных (обеспечивает хранение информации, поступающей в систему) модуль корреляции (осуществляет корреляцию собранных данных); модуль автоматизации УИИБ (осуществляет автоматизацию процессов УИИБ) агенты (собирают информацию непосредственно с устройств). В состав системы также входят средства по написанию агентов сбора данных из нестандартных систем защиты, средства формализации пользовательских правил корреляции и создание отчетов.

Для описания процедуры УИИБ согласно [1, 7] можно использовать классическую модель непрерывного улучшения процессов, получившая название от цикла Шухарта-Деминга - модель PDCA (планируй - «Plan», выполняй - «Do», проверяй - «Check», действий - «Act»). Стандарт [1] описывает модель PDCA как основу функционирования всех процессов системы управления информационной безопасностью. Эта модель объединяет 4 взаимосвязанных процесса: разработка, внедрение, мониторинг и развитие. Жизненный цикл системы управления будет определяться следующими этапами: 1) Планирование и подготовка. Осуществляется разработка схемы УИИБ, разработка и утверждение ряда организационно-регламентирующих документов, выделение человеческих и материальных ресурсов, проведения необходимого обучения и апробация выбранной схемы управления. 2) Эксплуатация. Осуществляется обнаружение и идентификация инцидента ИБ, реагирования, расследования и анализ. 3) Анализ. Осуществляется анализ системы управления инцидентами информационной безопасности, выявляются участки по улучшению и меры по улучшению. 4) Улучшение. Реализуются рекомендации, разработанные на этапе анализа. В общем, эта процедура регулируется стандартом [1], пришедший на смену BS 15000: 2002, который, в свою очередь, взял за основу библиотеку ITIL. Следует отметить, что все стандарты ISO / IEC серий 9000, 14000, 20000, 27000 и др., описывают правила создания систем управления различными процессами, гармонично сочетаются друг с другом, и в качестве основы управления подконтрольными процессами используют процессный подход, который рассматривает управление как процесс, то есть как набор взаимосвязанных непрерывных действий. Процессный подход акцентирует внимание на достижении поставленных целей, а также на ресурсах, затраченных для этого.

Процесс УИИБ, как правило, возлагается на службу ИТ-поддержки, которая обрабатывает инциденты ИБ (в случае, если такая служба существует в организации). Это еще раз доказывает факт целесообразности разработки единой системы управления всеми процессами в компании, так как управление подобными процессами в различных отраслях ее деятельности часто выполняется по одной схеме. Стоит также понимать,

что УИИБ НЕ предупреждает нанесения ущерба компании, однако расследование инцидента ИБ и своевременное внедрение превентивных и корректирующих мер снижает вероятность его рецидива. Работа организации без СУИИБ может обернуться рядом проблем. В результате внедрения процесса управления проблемами организация получает такие важные и полезные свойства как качество сервисов, сокращение числа инцидентов и непрерывного функционирования. В условиях роста влияния ИТ на деятельность современных организаций, значительное внимание уделяется организации поддержки и сопровождения ИТ-систем. Мировой опыт по управлению ИТ-организациями и их взаимодействием с заказчиками описан в, упомянутой ранее, библиотеке ITIL. Она содержит комплекс необходимых для построения СУИИБ рекомендаций. Во-первых, в ITIL с определенной степенью детализации описан процесс управления безопасностью (Security Management). Во-вторых, предоставление ИТ-услуг, включая сервисы ИБ, относится к ответственности служб ИТ и ИБ организаций. Для эффективного расследования инцидентов ИБ необходимы не просто дифференцированный инструментарий, а специализированный унифицированный комплекс таких инструментов, так называемый toolkit. Необходимость соблюдения требований стандартов, а также законов о проведении расследований, накладывает определенные сложности в работе следователей, приводит к накоплению неструктурированных данных, а также увеличивает расходы на проведение расследования. Все это стало основой разработки интегрированных специализированных наборов инструментов для проведения расследований, включающих в себя такие возможности как анализ смартфонов, мобильных телефонов, распределенные вычисления, планирование задач и тому подобное. То есть, основными требованиями, для эффективного проведения расследований инцидентов, должны быть интегрированность всех инструментов, распределение вычислений, оперирования большими объемами данных без сбоев, оперативное выявление попыток вторжения и уязвимых мест ИКС, возможность расширения функционала, создание детализированных отчетов, быстрый доступ к связанным данным, а также возможность взаимодействия с другими группами CERT/CSIRT. Также, для повышения вероятности идентификации злоумышленника, отслеживания активности и выявления его истинных намерений следует проводить анализ сетевой активности и осуществлять визуализацию информационных потоков.

Выводы. Таким образом, анализ научно-методических и нормативно-правовых источников показал необходимость и позволяет систематизировать теоретические основы разработки СУИИБ. В работе также определены фазы жизненного цикла инцидента ИБ и приведены компоненты типичной СУИИБ. Эффективное функционирование позволит аккумулировать информацию об инцидентах ИБ, категоризировать их и определять наиболее актуальные угрозы и, как результат, максимально

эффективно внедрять превентивные меры, что позволит повысить уровень защищенности ИКС организации в целом.

Использованные литературы

1. O‘z DSt ISO/IEC 27001:2016 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.
2. O‘z DSt ISO/IEC 27035:2015 Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности.
3. Альтерман Б. Д., Дрожжинов В. И, Моисеенко Г. Е. Обеспечение непрерывности деятельности организации в нештатных ситуациях // Jet Info, 2003. № 5.
4. Пошаговое руководство по созданию CSIRT (Европейское агентство по сетевой и информационной безопасности (ENISA) в рамках программы WP-2006), 2006. — 86 с.
5. Moira J.W.-B. Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J.W.-B., Stikvoort D., Kossakowski K.-P. et al. — Pittsburgh, 2003. — 223 p.
6. European Network and Information Security Agency [Electronic resource]: ENISA. — Electronic data. — Heraklion, Greece: ENISA, [04.02.2012]. — Mode of access: World Wide Web. — URL: http:// www.enisa.europa.eu. — Description based on screen.
7. Липунцов Ю. Прикладные программные продукты для экономистов. Основы информационного моделирования. Учебное пособие. – Litres, 2017.