Management information base of cybersecurity
Gusnin S.[1], Petukhov A.[2]

Информационная база управления кибербезопасностью
Гуснин С. Ю.[1], Петухов А. Н.[2]

[1]Гуснин Сергей Юрьевич / Gusnin Sergey – кандидат технических наук, доцент,
кафедра информационных и сетевых технологий,
Институт информационных систем и технологий,
Московский авиационный институт
Национальный исследовательский университет;
[2]Петухов Андрей Николаевич / Petukhov Andrey – кандидат технических наук, доцент,
кафедра информационной безопасности,
Московский институт электронной техники
Национальный исследовательский университет, г. Москва

Аннотация: *в статье анализируется текущая ситуация в сфере управления информационной безопасностью. Рассматриваются подходы к построению информационной базы управления безопасностью. Указывается, что информационная база управления безопасностью обязательно должна иметь проактивный, пассивный и реактивный аспекты представления об опасности. Используемые структуры данных и средства накопления информационной базы управления безопасностью должны работать с реестрами различных информационных активов, развитыми форматами описания угроз и технологий их реализации, а также с представлением факторов снижения информационных рисков. Работы по сбору и анализу данных для информационной базы управления требуют привлечения двух видов компетенции: общей методической в области информационной безопасности и специальной в области организации информационных технологий в конкретной индустрии.*

Abstract*: the article analyzes current situation in thearea of information security management. It discussest hewaystobuild security management information data base; tells that security management information data base must have proactive, passive and reactive aspects of performance about thedanger.Used data structures and ways of accumulation of security management information data base must work with registers of various information actives, developed threat descriptions and technology of their implementation, with factors of information risks decrease. Works on collecting andanalyzing data forin formation management data base require attraction two types of competence: General training in the field of information security and special in the field of organization of information technologies in specific industry.*

Ключевые слова: *информационная безопасность, управление, база данных, технологии реализации угроз, инвариантность сегментирования киберпространства, политика безопасности.*

Keywords: *information security, management, database, technology implementation threats, invariance segmentation of cyberspace security policy.*

.

Обсуждение положения с безопасностью обращения информации в разных областях человеческой деятельности (не только технических) показывает, что на фоне действующих (и весьма эффективно) методов и инструментов защиты от киберугроз практически отсутствует согласующий элемент – управление безопасностью. В распоряжении потребителей информации есть переполняющая рынок индустрия программно-технических решений, которые декларируют всевозможные контроли и учеты, ограничения доступа к информации на всех мыслимых уровнях, фильтрации всех видов трафика, неизбежного обнаружения любого вредоносного кода. Это разнообразие дополнено богатым потенциалом настроек и конфигурирования (включая интеграцию в инфраструктуру), а также широким ассортиментом средств отчетности. И, тем не менее, не снижается острота вопросов «а что со всем этим делать?», «какие средства и как использовать?», «какие параметры настроек устанавливать сначала и как их изменять потом?», «какие регистрационные данные полезны и как их использовать?» и многие другие, относящиеся к конкретным реализациям информационных процессов и технологий. Это вопросы различных уровней управления безопасностью и настоящая статья посвящена организации информационной работы в рамках такого управления.

Сегодня основная проблематика обеспечения безопасности неуклонно перемещается из области создания высокоэффективных программно-технических средств, криптостойких алгоритмов и интеллектуально насыщенных эвристических методов в область разработки и внедрения комплекса политик разного уровня, контроля их выполнения и обеспечения своевременной коррекции. Безопасность в таких индустриях как, например, гражданская авиация, является доминирующим фактором и уже не ограничивается внутригосударственной локализацией. Прошедшая в текущем году

сессия Международной организации гражданской авиации (ИКАО) была посвящена, в частности, кибербезопасности и показала, что для управления явно не хватает сведений и представлений. Поэтому один из основных векторов усилий в области безопасности эта организация усматривает в актуализации сведений о факторах и решениях безопасности. Итоговая декларация почти полностью посвящена аспектам поддержания полноты и адекватности представлений о том, что происходит в сфере кибербезопасности [1]. Этот пример показывает, что внимание начинает переключаться со средств на цели.

Целенаправленное обеспечение безопасности (любой) предполагает наличие адекватного представления об опасности. Поэтому начинать следует именно с него, с такого представления. В любом конкретном случае есть специфика структуры и формы этого представления, но общими элементами всегда являются:

- типология проявления опасности, номенклатура идентифицированных и квалифицированных видов такого проявления, внешних (агрессивность среды) и внутренних (несовершенство объекта) событий и ситуаций, являющихся причиной возникновения ущерба (проактивный аспект);
- совокупность и структура активов (объектов и процессов), подвергающихся опасности, в нашем случае речь идет о пространстве информационных ресурсов, их состояний и взаимодействий, а также о характере их подверженности опасности (пассивный аспект);
- элементы и свойства объекта (средства защиты, особенности архитектуры, ограничения и т.п.), препятствующие реализации опасности (реактивный аспект).

Для осмысленного управления в любой области необходимо обладать знанием о целях, факторах среды, текущем состоянии объекта, инструментах управления и др. В нашем случае эти знания должны содержать, как минимум, инвентаризацию информационных активов (ресурсов и процессов), сведения об агрессивном потенциале среды и каналах его реализации, а также представление о реальных возможностях мер противодействия (т.е.). Это те самые упомянутые проактивный, пассивный и реактивный аспекты, т.е. информационная база управления безопасностью практически совпадает (с точностью до критериев, внесистемных факторов и ресурсных ограничений) с представлением об опасности.

Следует отметить, что одна из базовых моделей управления рисками безопасности – трехдольная модель с полным перекрытием (или она же, дополненная вероятностными мерами - модель Клементса-Хоффмана [2]) - основана именно на этих информационных агрегатах. На базе таких сведений строится собственно модель угроз, проводится анализ и управление рисками, исследуются уязвимости, учитываются инциденты, и, самое главное, эти данные используются при формировании политик безопасности.

Каноническая триада «что, от чего и чем защищаем», так или иначе, упоминается во всех пособиях по управлению информационной безопасностью и приобрела уже некоторый оттенок банальности, но практическое воплощение ее далеко не идеально. Обычно ее декларирование и поддержание относят к верхнему (стратегическому) уровню управления и определяют в концепции безопасности (политике верхнего уровня). В большинстве случаев эти документы носят формальный и одномоментный характер, инвентаризация активов сводится к указанию на нормативную категорию (персональные, конфиденциальные, банковские и т.п.), угрозы перечисляются в виде рубрик классификаторов, а потенциал противодействия – в виде перечня программно-технических сервисов. Детализировать управленческие воздействия, т.е. формировать политики более низкого уровня на основе таких сведений не просто, организовать циклический процесс непрерывного управления еще сложнее.

Есть, по крайней мере, еще одна причина для формирования информационной базы управления безопасностью. Знания о потребностях и возможностях защиты существуют и используются в конкретных процедурах и технологиях. Было бы безрассудным пытаться подправить что-то в этих местах без тщательного и глубокого анализа существа дела и его эффективности, как самого по себе, так и во взаимодействии с соседями. Но для проведения такого анализа необходимо сконцентрировать знания о факторах безопасности в этих процедурах и технологиях.

Создать и формализовано представить эти сведения сразу в полной, адекватной и конструктивной форме в рамках однократного проекта невозможно**.** Прежде всего, в силу большей или меньшей динамичности всех факторов безопасности (и среда, и объект управления, и возможности по защите развиваются). Поэтому давно уже утвердилась концепция процессного характера управления безопасностью. Но даже, если бы предметная область была бы статична, знания о ней в части перечисленных аспектов «рассеяны» по многочисленным источникам, и можно лишь организовать (запустить и поддерживать) процесс сбора таких знаний, обеспечив эффективное начальное состояние процесса и более или менее интенсивную его сходимость. Динамика предметной области делает такую сходимость проблематичной.

Кроме того, административная разобщенность носителей этих знаний затрудняет их сбор и интеграцию, поэтому целесообразно запустить процессы в пределах лишь части пространства

информационных взаимодействий, искусственно ограничив ее, и предпринимать попытки распространить эти процессы только после их отработки на первоначальном фрагменте.

Одним из существенных препятствий реализации такого подхода является естественная боязнь вычленить какие-то подсистемы, утратив при этом целостность, потерять из поля зрения какие-то взаимодействия («гиперсистемный подход»). Но сегодня в рамках диалектики определения и ограничения защищаемого пространства традиционная ущербность вычленения элемента из системы («ощупывание слепыми слона») частично компенсируется методической инвариантностью сегментирования киберпространства. Дело в том, что в современном предмете информационной безопасности все труднее определить границы, отделяющие потенциально опасные пространства. Виртуализация инфраструктуры, облачные вычисления, безузловые сети – все эти направления развития технологий сопровождаются некоторой утратой четкости такими понятиями как, например, «место обработки» или «траектория передачи». Узел и маршрут уступают место среде, а той в свою очередь на смену приходит пространство. Соответственно этому эволюционирует и информационная безопасность (в случае пространства – кибербезопасность), уже все труднее оперировать понятиями «источник угроз», «контролируемая зона», «доверенная среда» или «внутренний и внешний нарушитель» (разумеется, это не относится к их нормативным дефинициям), т.е. теми понятиями, которые включают детерминированные координаты. Таким образом, взгляд на предмет безопасности становится все более однородным.

Поэтому методическая инвариантность сегментирования киберпространства для анализа факторов безопасности состоит в том, что вычленять все равно что-то надо (нельзя объять необъятное), а дефектность такого вычленения будет примерно одинакова в силу «однородности» киберпространства. И центр тяжести при оценке эффективности модели перемещается от ее полноты к корректности интерфейса между выбранным сегментом и остальной частью киберпространства. Проблемы выбора достаточно «представительного» начального фрагмента киберпространства и ошибок адекватности от замены «внутренности» на интерфейс остаются, но их значимость неуклонно сокращается в процессе расширения модели.

В рамках уже упомянутой сессии IKAO среди прочих инициатив обсуждалась «Эталонная архитектура среды для разработки будущих бортовых систем» (FACE). Так вот в части безопасности она уже в структуре проектируемых систем предполагает использование интерфейсов, которые препятствуют распространению угроз и обеспечивают более или менее автономный анализ факторов безопасности внутри пространств между такими интерфейсами [3]. Другим примером может служить управление конфигурацией с помощью интерфейсов в сотовых сетях с функциональным закреплением каналов (3G) [4]. Возможно, соединение при таком управлении будет установлено на неидеальном (просто рациональном) маршруте, но это установление не потребует решения многомерной задачи оптимизации.

Но надо быть готовым, к тому, что процессы, успешно функционирующие только в отношении ограниченной части информационного пространства не дадут возможности сформировать полноценные политики. Этот результат можно получить только на основе полностью интегрированных знаний обо всех участниках информационной деятельности, и тогда можно выходить на стратегический уровень управления (например, вплоть до общей концепции информационной безопасности в отрасли).

Структуры данных и средства накопления информационной базы управления безопасностью должны позволить работать с реестрами различных информационных активов, например, с альбомами протоколов обмена или структурами кадра в канале обмена. И здесь очень важным является вопрос детализации данных. С одной стороны избыточная детализация вредна с ресурсной точки зрения и, возможно, из соображений секретности. С другой – есть риск за интегрированностью данных упустить реальную уязвимость. Этот вопрос требует пристального внимания, и на начальном этапе может быть решен в пользу более интегрированного вида с возможностью последующей детализации. Есть де-факто стандартизованные решения для таких данных, например, классификаторы конфигураций и уязвимостей германского BSI [5]. Возможность их непосредственного применения во всех случаях сомнительна, но использование в качестве ориентира может быть весьма полезно.

Сам вид сведений о реальных угрозах вместе с характером информационных инфраструктур и идеологией обеспечения безопасности в процессе эволюции претерпел принципиальные изменения. На первоначальных этапах защиты информации акцент делался на типологию деятельности злоумышленника и используемые классификаторы были достаточно конструктивны, чтобы выбрать номенклатуру сервисов безопасности. Сегодня в условиях многоэтапных атак с обязательной преамбулой подготовки и вероятным последующим уничтожением следов, указание на тип нарушения без анализа контекста уязвимостей, технологий и каналов реализации и атак становится малоконструктивным. Поэтому отдельного упоминания заслуживает разработка форматов и средств хранения и анализа собираемых и накапливаемых сведений об угрозах. Пример таких баз данных есть,

например, база угроз и уязвимостей на сайте ФСТЭК РФ, включающая описание атак, реализующих каждую уязвимость [6].

Существует не менее десятка эффективных и практически апробированных методик сбора и анализа сведений о реальных угрозах как на основе уже свершившихся инцидентов, так и на базе средств оценки защищенности. Эти методики в конкретном случае, возможно, нуждаются в большей или меньшей адаптации, но это уже существующая платформа, с которой можно начинать.

Практически в любой отрасли есть виды деятельности, непосредственно определяющие информационно-технологические процессы, это работы по созданию информационных технологий: проектирование, разработка, тестирование и внедрение различных программно-технических средств, комплексов и систем. Характер проявления угроз безопасности на этапах проектирования и эксплуатации несколько отличаются и есть специфика проектной деятельности в части инвентаризации факторов безопасности. Возникает как бы два вида активов – с одной стороны это сами проектные решения, а с другой - процедуры их принятия и реализации. Это обстоятельство рельефно проявляется в «Общих критериях» [7] , где требования безопасности разделены на функциональные и требования доверия. Поэтому анализ факторов проектирования, разработки и внедрения, влияющих на безопасность, должен быть самостоятельным вопросом управления безопасностью.

При организации процессов сбора данных необходимо также решить ряд обеспечивающих вопросов, в частности, сохранения действующих и апробированных методов и приемов, проблему обеспечения секретности при концентрации сведений, создания комплексной компетенции.

Сама по себе концентрация знаний не должна влиять существующий уровень безопасности, поэтому надо сохранить весь потенциал реализованных решений, методов, правил, инструментов. Таким образом, сбор сведений сам по себе не должен вносить изменения и, тем более, носить нормирующий характер.

Практически все этапы работы по сбору и анализу данных для информационной базы управления требуют привлечения двух видов компетенции: общей методической в области информационной безопасности и специальной в области организации информационных технологий в конкретной индустрии. Такой компетенции в комплексе, скорее всего, либо совсем нет, либо ее ресурс весьма ограничен. Поэтому в планах работ необходимо предусмотреть обучение персонала, участвующего в процессах сбора сведений о факторах безопасности.

Действия по сбору и анализу данных это еще не строительство здания управления безопасностью, это лишь попытка завезти на строительную площадку материалы и сделать так, чтобы они не пропали. А для строительства дома надо выполнить дальнейшие действия:

- закрепление, поддержание и развитие процессов сбора информации;
- анализ рисков, разработка политик;
- внедрение и контроль исполнения политик;
- запуск цикла управления безопасностью;
- мониторинг событий безопасности при эксплуатации: регистрация, нормализация и корреляция событий, привлечение технологий управления инцидентами.

Литература

1. 39-я сессия Международной организации гражданской авиации «Решение проблем кибербезопасности в гражданской авиации». A39-WP/17 EX/5 30/5/16.
2. *Хоффман Л. Д.* Современные методы защиты информации // Л. Д. Хоффман; под ред. В. А. Герасименко. М.: Сов. радио, 1980. 264 с.
3. Технический стандарт «Эталонная архитектура «Среда поддержки будущих бортовых систем FACE™ (FutureAirborneCapabilityEnvironment)». Издание 1.0 ISBN:1-937218-04-1. Номер документа: C122. Опубликован OpenGroup, январь 2012 г.
4. *Невдяев Л. М.* Мобильная связь 3-го поколения. // Серия изданий «Связь и бизнес». М., 2000. 2008 с.
5. ITBaselineProtectionManual.Standardsecuritysafeguards. [Электронный ресурс]. Режим доступа: http://www.bsi.bund.de/gshb/english/menue.htm/ (дата обращения: 13.04.2009).
6. Банк данных угроз безопасности информации. [Электронный ресурс]. Режим доступа: http://www.bdu.fstec.ru/ (дата обращения 21.11.2016).
7. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.