ТЕЗИСЫ ДОКЛАДОВ

Научно-практической конференции-совещания

«Методы и средства обеспечения информационной безопасности (кибербезопасности) АСУ ТП»

17 февраля 2016 г. Москва, ИПУ РАН

ТЕРМИНОЛОГИЯ БЕЗОПАСНОСТИ. КИБЕРБЕЗОПАСНОСТЬ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Алпеев Анатолий Степанович, к.т.н., ФБУ «НТЦ ЯРБ»

Понятие «безопасность» в современном мире играет едва ли не самую главную роль во всех жизненных процессах: биологических, политических, экономических, социальных, технических, территориальных и др. Поэтому очень важно не только корректно определять это понятие и его производные, но и правильно применять их по назначению. К сожалению, к настоящему времени этот весьма желаемый результат не получен. Однако попытки его достижения продолжаются.

В этой статье рассматриваются сравнительно недавно появившиеся термины «Кибербезопасность» и «Информационная безопасность», определение которых, и их производных, на мой взгляд, выполнены не совсем корректно. Поскольку важность этих понятий в современном мире очень велика, то их анализ и предложения по корректировке заслуживают пристального внимания.

В качестве критикуемых определений термина «кибербезопасность» в этой статье взято определение этого термина из [1]:

«Кибербезопасность - условия защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться не желательными».

И определение этого термина из [2]:

«Кибербезопасность – совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями».

При рассмотрении этих определений в первую очередь хочется отметить неправомерный выбор в них родового термина: «условия» из [1] и «совокупность условий» из [2], поскольку сам термин указывает на необходимый родовой термин: «безопасность». Это говорит о том, что термин «кибербезопасность» является производным от родового термина «безопасность», таким образом, что «кибербезопасность» представляет собою часть понятия «безопасность», выделяемую некоторыми специфическими особенностями, которые должны составить вторую часть определения термина «кибербезопасность» следующую за родовым словом. Поскольку родовое слово в выбранных определениях термина «кибербезопасность» выбрано не правомерно, то обсуждать вторую часть этих определений не целесообразно. Дальнейшие соображения по поводу определения термина «кибербезопасность», связаны с выбором определения термина «безопасность», который бы позволил корректно сформировать вторую часть определения термина «кибербезопасность», следующую за родовым словом.

В этой статье для этой цели выбрано определение «безопасность» из [3]:

«Безопасность - наука, изучающая природные, техногенные, социальные, экономические и другие процессы образования, развития и взаимодействия субъектов, объектов, окружающей среды и их комбинаций с целью выявления источников опасностей,

определения их характеристик и формирования законов и других нормативных актов, устанавливающих понятия, требования, рекомендации и методики, выполнение которых должно гарантировать защищенность интересов отдельной личности и общества в целом от всех выявленных и изученных источников опасности».

В [3] проведен анализ причин, по которым выбрано это определение и предложены методы формирования других понятий, связанных родовыми отношениями с термином «безопасность». Пользуясь этим методом формирования определений, предлагается следующая формулировка термина «кибербезопасность»:

Кибербезопасность – раздел безопасности, изучающий процессы формирования, функционирования и эволюции киберобъектов, с целью выявления источников киберопасности, которые могут нанести им ущерб, и формирования законов и других нормативных актов, регламентирующих термины, требования, правила, рекомендации и методики, выполнение которых должно гарантировать защищенность киберобъектов от всех известных и изученных источников киберопасности.

Под киберобъектом здесь понимается, любой объект, функционирование которого осуществляется с участием программируемых средств.

Заметим далее, что определение термина «кибербезопасность» из [1, 2] базируется на понятии «киберпространство»:

«Киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)» из [2].

В определении термина «киберпространство» также родовой термин «сфера» выбран не логично. Этот термин был бы уместен, если бы определялся термин «киберсфера». На мой взгляд, более корректно определить понятие «киберпространство» через понятие «киберобъект» следующим образом:

Киберпространство – пространство, в котором осуществляется функционирование и взаимодействие киберобъектов.

В соответствии с рекомендациями [3], далее следует определить термин «кибербезопасность объекта» как внутреннее свойство объекта не быть опасным для окружающей среды при его функционировании во всех режимах работы:

Кибербезопасность объекта – свойство объекта, характеризующее его внутренние возможности не быть причиной образования ущерба для внешней среды или ограничивать его величину допустимыми нормами.

При этом следует понимать, что ущерб киберобъекту наносится в результате специально организованных кибератак. Под кибератакой в этой статье понимается – предумышленно организованная совокупность действий с участием программно технических средств (ПТС), направленная на нанесение экономического, технического или информационного ущерба. Например, получение секретных сведений по различным аспектам.

По источнику организации кибератаки можно подразделять на две группы: внешние, по отношению к объекту кибератаки и внутренние. Так, например, в [4] описан случай организации внутренней кибератаки с корыстной целью заработать деньги.

«Первым хакером в истории СССР оказался простой программист Мурат Уртембаев, которому прочили блестящую карьеру математика в МГУ, но он отказался от научной стези, и по целевому распределению попал на АВТОВАЗ. Там его таланты никто не оценил, и он решил доказать, что чего-то да стоит. Схема работы была следующей - программист, если считал нужным, вносил изменения в ПО, но не оставлял никаких данных или отметок о внесенных изменениях. Мурат смекнул, что можно без труда «хакнуть» систему, и никто его не спалит. В ходе проверки выяснилось, что первый хакер СССР был первым пойманным, но отнюдь не первым, кто обнаружил окно в системе, и «хакнул» ее. В том же Управлении, в котором работал Уртембаев, «элита» регулярно создавала сбои на конвейере и оперативно их ликвидировала, выбивая у начальства за спасение конвейера в качестве награды дачи, квартиры, автомобили».

Таким образом, источником внутренней кибератаки может быть персонал объекта кибератаки или персонал имеющий доступ к его программному обеспечению, если за действиями этого персонала нет должного контроля.

Случаи внешних кибератак описываются довольно часто, особенно на сети банков и финансовых организаций с целью присвоения денег с чужих счетов и карт частных пользователей. Однако уже имеются случаи кибератак на АЭС, например, в [5] «глава Организации пассивной обороны Ирана Голям Реза Джалали заявил, что иранские специалисты завершили расследование обстоятельств кибератаки. Согласно его результатам, вирус Stuxnet, атаковавший Бушерскую АЭС, запустили из Израиля и американского штата Техас. Также Джалали высказал предположение, что инжиниринговая корпорация Siemens, которая поставила и установила на АЭС систему сбора и обработки данных SCADA, также причастна к атаке. Концерн, по мнению составителей доклада, должен объяснить, почему он предоставил «врагам» Ирана коды SCADA, в результате чего и стала возможной кибератака. В конце сентября иранским программистам удалось справиться с компьютерным вирусом, который, по утверждениям главы Организации по атомной энергии Ирана Али Акбара, находился в нескольких ПК, принадлежащих сотрудникам АЭС».

В [5] указывается также, что «Сейчас группа специалистов (или даже одиночка) способны с помощью технических и информационных средств нанести непоправимый вред военной, экономической, технологической, политической и информационной безопасности любого государства. Поэтому большинство действий, осуществляемых сторонами в кибервойне, влияет на межгосударственные отношения и может привести к политическому противостоянию».

В качестве критикуемых понятий «Информационная безопасность» в статье взяты следующие понятия:

«Информационная безопасность — защита конфиденциальности, целостности и доступности информации» из [6].

«Информационная безопасность – состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве» из [2].

Сложность этого понятия состоит в том, что сам предмет, безопасность которого определяется, не определен как по внутренней структуре, так и по внутренним свойствам, которые необходимы для формирования требований к его безопасности. Даже само определение информации, в настоящее время весьма не однозначно и противоречиво. Таким образом сформировать понятие безопасности такого предмета на основании его внутренней структуры и внутренних свойств не представляется возможным.

Тем более что к определению из [2] даны определения указанных в нем составляющих:

Конфиденциальность информации - такое состояние информации, при котором доступ к ней только у объектов с наличием прав на нее.

Целостность информации - блокировка несанкционированных изменений информации.

Доступность информации - избежание сокрытия информации от пользователей с правами доступа.

Обращает внимание то, что все составляющие представляют собой только внешние действия по отношению к информации: назначение прав доступа к информации; блокирование несанкционированных изменений информации; избежание сокрытия информации от пользователей с правами доступа.

К тому же, хочется отметить то, что оба взятых для критики понятия фактически устанавливают эквивалентность терминов «безопасность» и «защищенность», что соответствует [7]. Сравните сами: в [1] «безопасность – защита» и в [6] «безопасность – состояние защищенности». С моей точки зрения, это совсем не так. Такая ситуация в терминологии именуется порочным кругом: «безопасность это защищенность», а «защищенность это безопасность». Но, как правило, защищенность объекта это его защита от внешних источников опасности, в то время как безопасность объекта это внутреннее свойство объекта не быть источником опасности для окружающей среды. С этой точки зрения следует различать два термина: «Кибербезопасность объекта» и «Киберзащищенность объекта», что соответствует в английской интерпретации «Cyber safety object» и «Cyber security object». Первый термин определен выше, второй термин, на мой взгляд, должен быть определен следующим образом:

Киберзащищенность объекта – свойство объекта, характеризующее его внешние возможности предотвращать образование ущерба от кибератак или ограничивать его величину допустимыми нормами.

Что касается термина «информационная безопасность», то имеет смысл пока рассуждать об информации как о черном ящике, т.е. только о защищенности информации. Поэтому термин «безопасность информации», на данный момент времени определяется только намерениями ее обладателя и ни чем другим.

Это дает основания утверждать, что термин «информационная безопасность» на данный момент времени (пока не определено корректно, что такое информация и какова ее

внутренняя структура и свойства) не корректен по своей сути. Вместо него можно предложить термин «информационная защищенность» и использовать для него определение изложенное ранее т. е.:

«Информационная защищенность — защита конфиденциальности, целостности и доступности информации», что, на мой взгляд, соответствует реальному состоянию рассматриваемой проблемы.

В заключении автор выражает надежду на то, что приведенная в статье аргументация поможет некоторым образом продвинуть понимание терминологии безопасности на качественно новый уровень.

Литература

[1] ISO/IEK 27032 2012. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».

[2] Концепция стратегии кибербезопасности российской федерации http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

[3] Ежемесячное приложение к журналу «Стандарты и качество». Экологические аспекты проблем надежности и безопасность технических систем. «Основные понятия безопасности». Алпеев А.С. М., 1994, вып. 7.

[4] Первый хакер в СССР. Остановил конвейер ВАЗа и остался на свободе/ http://yandex.ru/yandsearch?lr=213&text=%D0%BF%D0%B5%D1%80%D0%B2%D1%8B%D0%B9+%D1%85%D0%B0%D0%BA%D0%B5%D1%80+%D1%81%D1%81%D1%81%D1%80&csg=5649%2C41594%2C12%2C25%2C3%2C0%2C0.

[5] Армейский вестник от 04.09.2012г. «Мировые кибервойны». http://lastbabylon.com/node/387.

[6] Википедия. https://ru.wikipedia.org/wiki Информационная безопасность

[7] Словарь русских синонимов.

ОПЫТ РАЗРАБОТКИ НОРМАТИВНОЙ ДОКУМЕНТАЦИИ ПО ИБ АСУ ТП АЭС

Бабаев Денис Игоревич, Московский филиал «Центратомтехэнерго» АО «Атомтехэнерго»

АЭС России являются стратегически важными объектами повышенной опасности. При этом в АСУ ТП современных АЭС повсеместно используются передовые цифровые устройства и технологии. Вместе с тем во всем мире происходит постоянный рост кибератак на АСУ ТП промышленных объектов. Методы, средства и тактика проведения подобных атак совершенствуются. Поэтому в настоящее время нарастает необходимость борьбы за информационную безопасность (далее ИБ) на АЭС России.

Работы по созданию нормативной базы в отрасли начались в 2011 году. Тогда была разработана «Программа по разработке дополнительных технических и организационных мероприятий по обеспечению информационной безопасности АСУ ТП». В 2014 году рамках указной программы были разработаны [1], в основу которых был положен [2]. 14 марта 2014 года приказом №31 ФСТЭК России утверждены [3].

В ноябре 2015 года на базе Московского филиала «Центратомтехэнерго» АО «Атомтехэнерго» (ЦАТЭ) начаты работы по созданию требований ИБ на этапах жизненного цикла АСУ ТП АЭС.

К указанным работам, помимо ЦАТЭ, были привлечены:

- специалисты ИПУ РАН;
- специалисты ЗАО «КРОК».

При разработке документов учитывались положения международной, иностранной и отечественной нормативной базы в части ИБ АСУ ТП, в том числе таких отечественных предприятий как ОАО «ГАЗПРОМ» и ОАО «РЖД».

В ходе выполнения работ были решены следующие задачи:

- определение уровня документов и выбран нормативный профиль;
- определен жизненный цикл АСУ ТП АЭС;
- разработаны требования к менеджменту ИБ АСУ ТП;
- определены требования к модели угроз и оценки рисков;
- сформированы принципы обеспечения ИБ АСУ ТП АЭС;
- разработаны требования к оценке рисков и выявлению угроз ИБ АСУ ТП АЭС;
- сформулированы требования к классификации элементов АСУ ТП по ИБ;
- введены требования к зональной модели АСУ ТП АЭС;
- разработаны требования к защищенному программированию;
- разработаны положения по проведению аудитов ИБ АСУ ТП;
- учтены аспекты ИБ, связанные с персоналом;
- требования гармонизированы со сложившейся практикой создания и эксплуатации АСУ ТП АЭС.

Разработка нормативной документации проведена в сжатые сроки (1 год). В итоге были разработаны два документа, отвечающие соответствующие современным международным и отечественным стандартам по ИБ.

Литература

[1] ОП 1.5.2.01.999.0205-2014 «Общие положения по обеспечению безопасности информации АСУ ТП на АЭС». ОАО «Концерн Росэнергоатом» № 9/77-П от 30 января 2014 г.

[2] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России приказом от 11 февраля 2013 г. №17

[3] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31

ЛОГИКО – АЛГЕБРАИЧЕСКАЯ СИСТЕМНАЯ КОНЦЕПЦИЯ МАТЕМАТИКИ И ЕЁ ПРИЛОЖЕНИЕ ДЛЯ СИНТЕЗА ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Бурлов Вячеслав Георгиевич, д.т.н., Санкт-Петербургский политехнический университет Петра Великого

Для синтеза модели процесса обеспечения информационной безопасности необходимо выделить модель объекта, модель действия и эти два элемента замкнуть между собой через эффективность применения (ЭП) системы. Введены три базовых понятия

Определение 1. Множество требуемых пространственно-временных состояний (ПВС) процесса обеспечения информационной безопасности $Q \subset R = X \times T$, называется район сосредоточения основных усилий (РСОУ) группировки в операции. ($Q = X^q \times T^q$ - декартово произведение) (Модель действия.).

Определение 2. ЭП есть свойство системы, которое характеризует степень реализации возможностей системы в процессе жизненного цикла. Оценивается показателем I(Q) в условиях ограничений.

Определение 3. Функцию $\varphi(r)=\Phi(u(r),v(r),r)$, где u(r), v(r), соответственно, вектора управления и возможностей, а $r \in Q$, будем называть потенциалом поля эффективности (ППЭ) разрабатываемой системы (Физически - ППЭ– производительность системы, распределённая в пространстве и времени. Модель системы, объекта).

Получено условие связи модели системы (объекта), модели действия системы (объекта) через показатель ЭП в форме

$$\int_{Q} \Phi(u(r),v(r),r)dr = I(Q). \qquad (1).$$

Такой интеграл есть алгебраическая операция f (r): $Q \Rightarrow R$ выбирает элементы $r \in R$, r =(x,t), пара пространство-время; удовлетворяющих уравнению синтеза (1) модели процесса. Физически эта операция "фильтрует" элементы множества R с целью выбора таких элементов, которые несут свойства создаваемой целевой системы и тем самым формируют элементы множества $Q \subset R$. Соотношение (1) – закон сохранения целостности[1]. Получены условия формирования структуры системы и распределения функций между ее элементами. (Множество G):

1. $X_{qi} \subset X_q$; 2. $X_{qi} \bigcap X_{qJ} = 0$, если $i \neq j$; 3. $\bigcup_{i \in J} X_{qJ} = X_q$, J = [1, N x M x H];

X^{qi} - требуемые пространственные состояния i - го элемента системы;

4. $\sum_{i \in J} \int_{T} (\Phi_i(u_i(t), v_i(t)) * X_{qi})\, dt = I$, где N, M, H -определяют количественный состав.

Определены вектора ПВС противостоящих сторон (А и Б) .

$$q_i^A = \langle x_{qi}^A, t_{qi}^A \rangle = \Theta_i^A((U^A, V^A, u^A(r), v^A(r)), (U^B, V^B, u^B(r), v^B(r));$$

$$q_j^B = \langle x_{qj}^B, t_{qj}^B \rangle = \Theta_j^B((U^B, V^B, u^B(r), v^B(r)), (U^A, V^A, u^A(r), v^A(r))).$$

В рамках разработанной методологии решены задачи следующих классов.

Задачи синтеза при заданном G

ЗАДАЧА С1. $\text{extr}\, I^A((U^A, V^A, u^A(r), v^A(r)), (U^B, V^B, u^B(r), v^B(r)))$.

$\text{extr}\, I^B((U^B, V^B, u^B(r), v^B(r)), (U^A, V^A, u^A(r), v^A(r)))$.

Задачи синтеза при не фиксированном множестве G и заданных U, V сторон

ЗАДАЧА С2. $\text{extr}\, I^A(G^A, G^B)$. $\text{extr}\, I^B(G^B, G^A)$.

Литература

1. Бурлов В.Г. Основы моделирования социально-экономических и политических процессов (Методология. Методы) СПб: Факультет Комплексной Безопасности, СПБГПУ.2007г.-265 с.

МЕТОД СИНТЕЗА МОДЕЛИ ПРОЦЕССА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Бурлов Вячеслав Георгиевич, д.т.н., Лепёшкин О.М., д.т.н., Санкт-Петербургский политехнический университет Петра Великого

Администратор безопасности формирует процессы обеспечения информационной безопасности. Основа формирования процесса (управления) – это решение администратора безопасности (ЛПР). ЛПР принимает решение на основе модели. [1]. Решение ЛПР должно содержать модель процесса, который он формирует (управляет). Модель должна быть адекватна программно-аппаратной среде функционирования информационной системы. Для обеспечения адекватности она должна базироваться на базовой закономерности предметной области.[2]. Базовой закономерностью предметной области является закон сохранения целостности (ЗСЦО).[2]. ЗСЦО -устойчивая повторяющаяся связь свойств объекта и свойств действия при фиксированном предназначении. Проявляется ЗСЦО во взаимной трансформации свойств объекта и свойств его действия при фиксированном предназначении.

В соответствии с ЗСЦ каждый процесс должен быть представлен тремя компонентами, соответствующими свойствам «объективность», «целостность», «изменчивость» (или «объект», «предназначение», «действие») по горизонтали. Тремя уровнями по вертикали в силу принципа трёхкомпонентности познания (Абстрактный, абстрактно-конкретный, конкретный). Или же в силу принципа познаваемости, базирующегося на трёх методах познания – декомпозиции, абстрагирования и агрегировании. Поэтому ЛПР, принимая решение оперирует стремя базовыми элементами в соответствии с понятиями «Объектом», «предназначением» и «действием» - это «Обстановка», «Выработка команды на нейтрализацию проблемы» (Реализация предназначения системы обеспечения безопасности) и «Информационно -аналитическая деятельность (ИАР)»; (Мониторинг).

В соответствии с такими рассуждениями мы оперируем следующими понятиями - **Управленческое решение (УР)**– обеспечение субъектом (администратором) условий реализации предназначения объекта, которым он управляет, в соответствующей обстановке; **Обстановка** – совокупность факторов и условий, в которых осуществляется деятельность; **ИАР** – непрерывное добывание, сбор, изучение, отображение и анализ данных об

обстановке. На рис. 1 представлена структурная схема основных этапов и элементов системного моделирования процесса построения модели **УР** ЛПР.

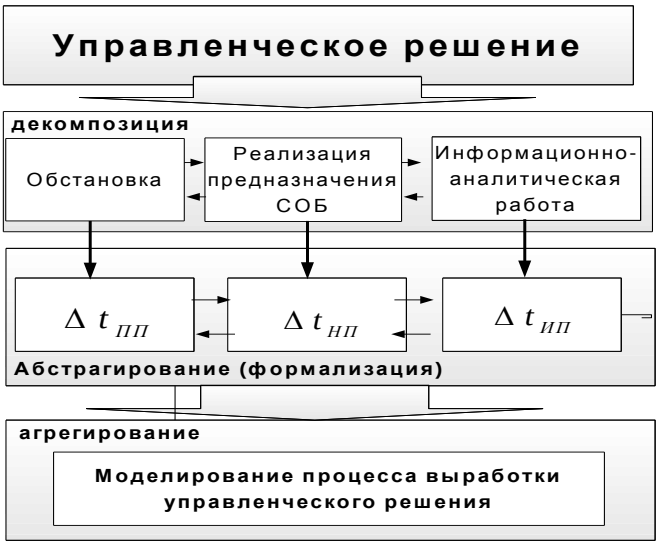

Рис.1. Структурная схема содержания процесса формализации **УР**

В результате применения методов декомпозиции, абстрагирования и агрегирования мы преобразовали понятие **УР** в агрегат – математическую модель **УР** следующего вида соотношение

$$P = F(\Delta t_{\text{ПП}},\ \Delta t_{\text{ИП}},\ \Delta t_{\text{НП}}) \qquad (1)$$

Где **Обстановке** соответствует характеристика периодичности проявления проблемы в информационной системе. **ИАР** соответствует среднее время идентификации проблемы в информационной системе. **Предназначению** соответствует среднее время нейтрализации проблемы. ***P*** вероятность того, каждая проблема, возникающая в системе, идентифицируется и нейтрализуется в рамках ограничений администратора. Так как только временные ресурсы невосполнимы, то характеристиками элементов **УР** являются такие элементы как, $\Delta t_{ПП} = 1/\lambda$ - среднее время проявление; $\Delta t_{ИП} = 1/\nu_1$ -среднее время идентификации; а $\Delta t_{НП} = 1/\nu_2$ среднее время нейтрализации проблемы. Схема управления в нашем случае имеет вид (рис 2.)

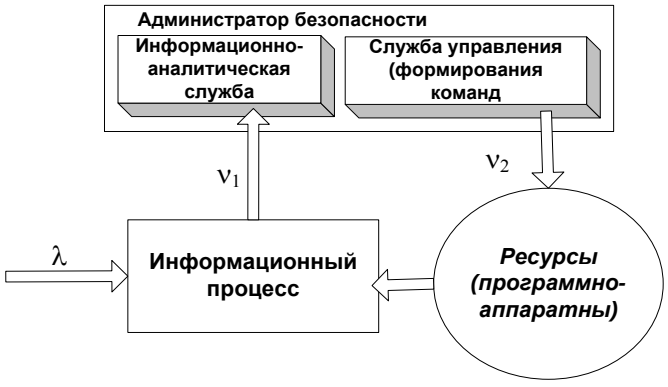

Рис.2. Структурная схема реализации **УР** администратора безопасности

Связь базовых элементов **УР** с показателем эффективности реализации УР администратора (1) конкретизируется системой дифференциальных уравнений. Задаваясь величиной *P,* в соответствии характеристикой обстановки λ , задавая по специальному

правилу парой ($\mathbf{v}_1$, $\mathbf{v}_2$), администратор всегда может обеспечить требуемый уровень безопасности.

Литература
1. Анохин П.К. Системные механизмы высшей нервной деятельности. М. "Наука", 1979, 453 с.
2. Бурлов В.Г. Основы моделирования социально-экономических и политических процессов (Методология. Методы) СПб: Факультет Комплексной Безопасности, СПБГПУ.2007г.-265 с.
3.Бурлов В.Г. Математические методы моделирования в экономике. Часть 1, -С-Пб. СПбГПУ, Факультет безопасности, НП «Стратегия будущего», 2007.- 330с.

К ПРОБЛЕМНОМУ ВОПРОСУ ОПИСАНИЯ ПОТЕНЦИАЛЬНЫХ УСЛОВИЙ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЭВОЛЮЦИОНИРУЮЩИХ СОЦИОТЕХНИЧЕСКИХ СИСТЕМ

Гудов Геннадий Николаевич, РГГУ, Рожнов Алексей Владимирович, к.т.н., ИПУ РАН

При проведении комплексных исследований актуальных проблемных вопросов обеспечения безопасности различного типа, а также планирования, анализа и контроля в системах управления силами и средствами при управлении безопасностью, в настоящее время приобретают немаловажное значение многосторонние исследования возможностей повышения эффективности мониторинга выполнения задач стратегического планирования [1].

В представленном докладе приводятся некоторые наглядные практики к описанию, с преимущественным использованием инструментальных средств [2], последовательности событий, приводящих к реализации угрозы, и наличию связей между этими анализируемыми событиями.

Разработанная модель реализации угроз [3], является обобщённой и вполне применима для описания событий совершения правонарушений и преступлений как для должностных лиц, имеющих допуск к защищаемой информации (внутренний нарушитель), в этом рассматриваемом случае не важно, сделал он это случайно (непреднамеренно) или сознательно (преднамеренно), так и для иных лиц, не имеющих допуска к защищаемой информации (внешний нарушитель).

Нарушитель своими неправомерными действиями или бездействием может нарушить безопасность информации или (и) создать условия к нарушению информационной безопасности путем [1, 3]: непреднамеренного воздействия на информацию носитель информации: случайно, ошибочно, из-за незнания требований нормативных документов, небрежного и халатного отношения к своим служебным обязанностям или вынужденные действия из-за психологического, морального, физического давления и т.п.; преднамеренного воздействия на информацию, носитель информации: осознанные действия, направленные на создание условий для изменения характеристик информационной

безопасности или (и) непосредственное разрушение характеристик информационной безопасности.

В аспекте многостороннего взаимодействия, этап возникновения дестабилизирующих факторов, создающих предпосылки для реализации угроз, предполагает возможность возникновения следующей последовательности важных событий [3]:

возникновение причин (мотивов), побуждающих (толкающих) к свершению правонарушений;

наличие обстоятельств, которые создает сам «нарушитель» осознанно или неосознанно;

создание условий, которые существуют или создаются на данном объекте защиты и способствуют совершению правонарушения и преступления.

На этапе создания дестабилизирующих факторов для реализации угроз должностное лицо или иного человека мы будем называть потенциальным нарушителем. И, в зависимости от действий нарушителя, выделим три ключевых этапа реализации угроз безопасности информации [1, 3].

1. Появление угрозы. На данном этапе будем считать нарушителя злоумышленником.

2. Проявление угрозы. На этапе проявления угрозы нарушителя будем относить к правонарушителям.

3. Реализация угрозы. На этапе реализации угрозы нарушитель становится правонарушителем, так как осуществляет конкретные противоправные действия, направленные на преодоление средств защиты.

В случае если правонарушителю всё-таки удается реализовать угрозу, которая нанесла ущерб безопасности информации, правонарушитель (по решению суда) признается преступником и ему определяют меру наказания.

Применение разобранного методического подхода позволяет определить (скорректировать предварительную оценку возможных рисков) угрозу совершения правонарушения на объекте защиты. В частности, с использованием данного подхода была предложена модель предупреждения конфликтов в среде радикалов, определены преобразования контейнеров среды радикалов, виды конфликтов для решения задачи исключения конфликта управления и сформирован метод обеспечения условий исключения конфликтов управления, позволяющий осуществить многосторонний комплексный контроль развития ситуации [2].

Литература

1. *Рожнов А.В*. О методических основах оценивания эффективности функционирования критичных социотехнических систем в сфере мониторинга и контроля государственного оборонного заказа / Труды 23-й Международной конференции "Проблемы управления безопасностью сложных систем" (Москва, 2015). М.: РГГУ, 2015. С. 338-342.

2. *Рожнов А.В., Лепешкин О.М., Гудов Г.Н.* Multidiscipline design environment based on radical-chart language / Seoul International Invention Fair 2012. Seoul, Korea: SIIF, 2012. С. 222.

3. *Гудов Г.Н., Рожнов А.В., Лобанов И.А., Купач О.С*. Методический подход к описанию сложных эволюционирующих систем при реализации угроз безопасности информации /

Труды XXI Международной конференции «Проблемы управления безопасностью сложных систем» (Москва, 2013). М.: РГГУ, 2013. С. 61-65.

ПОСТРОЕНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИБ АСУ П И ТП С ИСПОЛЬЗОВАНИЕМ ПАК DATAPK

Домуховский Николай Анатольевич, ООО «Уральский центр систем безопасности»

В докладе рассматривается классификация АСУ ТП атомной электростанции в соответствии с документом МАГАТЭ «Компьютерная безопасность на ядерных установках» с точки зрения различия требований по обеспечению ИБ различных классов АСУ ТП.

В докладе акцентируется внимание на необходимость учета критичности функционирования АСУ ТП при разработке мер по обеспечению ИБ, в том числе, о возможном влиянии системы обеспечения ИБ на корректность функционирования защищаемой АСУ ТП.

В докладе приводится подход к построению гибкой системы обеспечения ИБ, влияние которой на АСУ ТП может варьироваться в зависимости от уровня важности системы для безопасности ядерной установки, текущего режима функционирования системы, ее архитектурных особенностей и пр. Рассматриваются стадии создания системы обеспечения ИБ и особенности их реализации для АСУ ТП различных уровней важности.

В заключении доклада рассматривается применение комплекса DATAPK при построении гибкой системы обеспечения ИБ как для наиболее важных для безопасности ядерной установки АСУ ТП, так и для менее важных систем, но имеющих больше точек интеграции со смежными системами и сервисами.

ОЦЕНКА КИБЕРБЕЗОПАСНОСТИ АСУ ТП, КАК СОСТАВНАЯ ЧАСТЬ ОЦЕНКИ СООТВЕТСТВИЯ ПРОДУКЦИИ, ПОСТАВЛЯЕМОЙ НА АЭС

Звонарев Александр Валентинович, АО «ЭНИЦ»

Аттестация оборудования важного для безопасности АЭС, проводится с целью подтверждения соответствия оборудования установленным требованиям, в том числе требованиям нормативных документов, носящих обязательный характер в соответствии с законодательством Российской Федерации.

Аттестация оборудования на этапе его изготовления проводится в рамках процедуры оценки соответствия, проводимой в соответствии с Федеральными нормами и правилами НП 071-06 «Правила оценки соответствия оборудования, комплектующих, материалов и полуфабрикатов, поставляемых на объекты использования атомной энергии»

Оценка соответствия требованиям по кибербезопасности на этапах изготовления и эксплуатации, как часть процесса оценки соответствия, позволяет опираться на международный, национальный и отраслевой нормативный базис по оценке соответствия на всех этапах жизненного цикла АЭС, что в свою очередь, делает возможным:

1. Гармонизировать требования по кибербезопасности с существующим нормативным базисом применительно к объектам использования атомной энергии;

2. Использовать процедуры оценки соответствия требованиям по кибербезопасности при проведении квалификации оборудования на действующих АЭС, включая процедуры документооборота, оформления и регистрации результатов;
3. Проводить работы по квалификации оборудования аттестованными специалистами, имеющими опыт работы по оценке соответствия;
4. Выполнять работы по оценке соответствия оборудования испытательными лабораториями, аккредитованными в системе Госкорпорации «Росатом».

МЕТОДЫ И МЕТОДИКИ ОЦЕНКИ И УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Полетыкин Алексей Григорьевич, д.т.н., ИПУ РАН

В докладе будут представлены методы оценки ущербов и общая методика расчета и управления рисками для промышленных объектов, обладающих развитой системой защитных барьеров от угроз различной природы. Материал иллюстрируется примером построения системы управления киберрисками.

ПОСТРОЕНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ВНЕШНЕГО СОПРОВОЖДЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ЗАЩИТЫ ОТ КИБЕРУГРОЗ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

Полетыкин Алексей Григорьевич, д.т.н., ИПУ РАН

Рассматривая обеспечение информационной безопасности промышленных объектов как мультидисциплинарную задачу, которую необходимо решать на всех этапах жизненного цикла, предлагается создавать автоматизированные системы внешнего сопровождения для объединения усилий специалистов различного профиля. Материал иллюстрируется примером.

ОБЗОР И СРАВНЕНИЕ ТРЕБОВАНИЙ ПО КИБЕРБЕЗОПАСНОСТИ АСУ ТП АЭС

Промыслов Виталий Георгиевич, к.ф-м.н., ИПУ РАН

В докладе рассмотрена взаимосвязь основных документов по кибербезопасности АСУ ТП АЭС. Обсуждаются предложения по новым стандартам кибербезопасности АСУ ТП АЭС международной электротехнической комиссии (МЭК).

СЕРВИС МОДЕЛИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ

Промыслов Виталий Георгиевич, к.ф-м.н., Масолкин Станислав Ильич, ИПУ РАН

В докладе будет представлен WWW-сервис по моделированию кибербезопасности, показаны примеры его использования при анализе и выборе архитектуры систем управления. Каждому участнику конференции будет предоставлен свободный доступ к сервису.

АКТУАЛЬНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ ПО КИБЕРБЕЗОПАСНОСТИ АСУ ТП

Шипулин Антон Сергеевич, ЗАО «КРОК инкорпорейтед»

В докладе будет освещена актуальность обеспечения информационной безопасности систем технологического управления с использованием технических средств ИБ. Обзор существующих специализированных и традиционных технических решений по кибербезопасности применимых в промышленных системах. Будут показаны как решения способные контролировать и обнаруживать информационные угрозы, так и решения способные предотвращать их. Будет уделено внимание условиям, и ограничениям применения средств.