ЗАДАЧИ ПЕРЕПОДГОТОВКИ И ОБУЧЕНИЯ ПЕРСОНАЛА СИТУАЦИОННЫХ ЦЕНТРОВ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ И РЕГИОНОВ

Башелханов И.В., Оладько В.С., Трусов Н.А.

Федеральное государственное образовательное бюджетное учреждение высшего образования «Финансовый университет при Правительстве Российской Федерации» (Финансовый университет), 125993, ГСП-3, Россия, г. Москва, Ленинградский проспект, 49, e-mail: greeceer@mail.ru

В настоящее время переподготовка и обучение персонала Ситуационных центров в условиях инновационных угроз и информационного коллапса приобретает принципиальное значение. Эффективность функционирования Ситуационных центров напрямую зависит от квалификации, знаний и умений дежурного персонала (операторов) и руководителей. Собирая и анализируя информацию о возникающих инцидентах, Ситуационный центр может стать объектом кибератаки злоумышленника. Поэтому для повышения безопасности и эффективности Ситуационного центра предлагается при подготовке персонала особое внимание уделять развитию знаний и практических навыков в области информационной безопасности и технологий защиты информации.

Ключевые слова: тело катастрофы, тело ЧС, нейминг угроз, защита информации, ситуационный центр, переподготовка персонала, обучение персонала, содержание рабочей программы, инцидент информационной безопасности, угроза

OBJECTIVES RETRAINING AND TRAINING STAFF SITUATION CENTRE OF INTEGRATED SECURITY FOR ENTERPRISES AND REGIONS

Bashelhanov I.V., Oladko V.S., Trusov N.A.

Nowadays retraining and training of personnel Situational centers in conditions of innovation and information threats of collapse becomes crucial. The effectiveness of the Situational centers depends on the skills, knowledge and abilities duty personnel (operators) and managers. Situation Centre that collects and analyzes information about emerging incidents may also become the object of intruder cyber-attack. Therefore, to improve the safety and efficiency of the Situation Centre is requested to staff pay special attention to the development of knowledge and practical skills in the field of information security and data protection technologies.

Key words: disaster body, naming threats, information security, situation center, retraining of personnel, training, content of the curriculum, information security incident, threat

Современные ситуационные центры, по нашему мнению, призваны комплексно рассматривать «тело катастрофы», «тело ЧС» [1] и принимать меры по нейминг [3], локализации и нейтрализации возникающих при этом угроз.

Если для локализация и нейтрализация угроз имеются, в большинстве случаев, стандартные решения, то с нейнингом угроз возникают большие трудности в связи с огромной ролью знания и информационного коллапса [2,4] (глубоким семантическим содержанием и запредельным разнообразием входящей информации). Способность руководства Ситуационного центра (СЦ), так и исполнителей СЦ в описанных условиях к нейнингу и селекции угроз безусловно предполагает наличие серьёзной базы переподготовки и обучения персонала комплексной безопасности.

Большинство аварий на АЭС и других критически важных объектах инфраструктуры, как показывает мировой опыт, происходит по вине операторов в предутренние часы из-за нарушения биологических суточных ритмов- десинхроноза.

Анализируя сложные АСУ ТП выдающиеся советские и российские эксперты Прангишвили И.В. и Амбарцумян А.А. подчёркивают: « В разных странах роль и обязанности оперативного персонала определяются по-разному. Так в США человек рассматривается не как виновник, а как источник ошибок,

причины которых кроются в недостатках технических решений, в проектировании средств управления без учёта человеческого фактора, в недостатках программы обучения и тренировки. Отмечается, что чем серьёзнее событие, тем больше требуется участие операторов в поддержании безопасности АЭС. В Германии выявление недостатков традиционных инструкций опирающихся на точный анализ событий, вследствие чего вырабатываются существующие инструкции для операторов. Новые инструкции по эксплуатации АЭС предусматривают не только возможность, но и необходимость вмешательства операторов в управление объектами в самых критических ситуациях. В Швеции принято активное вмешательство оператора в ход аварии. При разработке аварийных управляющих процедур в качестве одной из задач ставят обеспечение правильности и полноты информации оператору, наличие избыточной информации… В отчёте INPO (США) подчёркивается, что 80% ошибок допущено обученным персоналом. Ошибки персонала специалисты INPO делят на ошибки в действиях (47%), недостатки в обучении (11%), неспособность следовать установленной инструкции (11%), а также неспособность выполнять не предусмотренные инструкцией задачи. Для операторов существенным оказывается то обстоятельство, что отказы, которые не обнаруживаются сразу, могут быть квалифицированы как обычная неисправность» [7].

Стратегическое планирование и стратегическое прогнозирование на сегодняшний день являются одними из наиболее востребованных направлений в области государственного управления, которые напрямую влияют на социально-экономическое развитие и обеспечение безопасности в масштабе целого государства. Как показано в [5,9] вопросы, связанные со стратегическим планированием и прогнозированием ситуаций часто решаются с помощью специализированных распределенных систем мониторинга и поддержки принятия решений, которые образуют государственные, ведомственные и региональные ситуационные центры.

Ситуационный центр представляет собой сложный гетерогенный высокотехнологический комплекс, включающий в себя телекоммуникационные системы и сети, системы информационно-аналитической поддержки, информационно-справочные системы, системы управления, реагирования и специального назначения, средства мультимедийного отображения информации и средства коллективной работы в режиме реального времени. СЦ может быть реализован на местном, окружном, региональном, межрегиональном и национальном уровне и для эффективного выполнения СЦ своих функциональных задач осуществлять информационный обмен с другими СЦ различного уровня и назначения. В соответствии с [6, 8] для информационного обеспечения в СЦ могут использоваться следующие источники:

- Федеральные органы исполнительной власти и их территориальные органы;
- Органы государственной власти субъектов РФ и их структурные подразделения;
- Центральные, региональные печатные и электронные СМИ;
- Независимые источники информации, агентства и службы;
- Ресурсы сети «Интернет».

Основными целью и задачами СЦ является:

- постоянный распределенный сбор и консолидация информации с различных источников в режиме реального времени;
- накопление и обработка полученных данных и их анализ;
- формирование событий и сценариев инцидентов;
- ранжирование по уровню важности и критичности ситуации;
- прогнозирование развития ситуации на основе анализа поступающей информации;
- принятие решений по каждой ситуации своевременное оповещение и оперативное реагирование на возникновение внештатных ситуаций.

Поскольку современные СЦ являются автоматизированными системами, требующими активное участие специализированного персонала для анализа поступившей в СЦ информации и адекватной реакции на возникшую ситуацию или инцидент, то на эффективность функционирования СЦ будет оказывать большое влияние качество подготовки и квалификация персонала СЦ: руководителя, специалистов, аналитиков, операторов, которые образуют дежурную смену СЦ.

В начале третьего тысячелетия информационная безопасность (ИБ) выходит на первое место в системе национальной безопасности Российской Федерации, это в первую очередь связано с тем, что на сегодняшний день, ряд государств открыто ведет информационное противоборство с Россией. В связи с этим более острыми становятся проблемы обеспечения безопасности личности, общества и государства от деструктивных информационных воздействий и кибератак. Поэтому формирование и проведение единой государственной политики в сфере ИБ требует приоритетного рассмотрения. Как показано в [10] одним из направлений разрешения этих проблем является подготовка кадров. Следовательно, задачами руководителя и персонала

дежурной смены СЦ является не только поддержание основных функций СЦ и адекватный своевременный анализ поступающих данных с учетом возможности возникновения инцидентов ИБ, но и обеспечение сохранности и безопасности информации СЦ, являющейся конфиденциальной. Поскольку сам СЦ также может представлять интерес и стать объектов целевой атаки злоумышленника. В связи с этим при подготовке и/или повышение квалификации персонала СЦ необходимо затрагивать вопросы и изучать дисциплины, связанные с обеспечением ИБ СЦ и своевременным выявлением инцидентов и событий ИБ.

Поэтому при подготовке специалистов и операторов СЦ предлагается изучать дисциплину «Основы информационной безопасности». Целью дисциплины является ознакомление обучающихся с основами ИБ, национальными интересами и угрозами ИБ Российской Федерации, с содержанием информационного противоборства на межгосударственном уровне, проблемами защиты информации и подходами к их решению. Задачи дисциплины направлены на формирование теоретического базиса и получение практических навыков в области вопросов информационного противоборства, основных угроз ИБ и способов реализации атак, законодательного, инженерно-технического, программно-аппаратного и организационного обеспечений ИБ, а также вопросов управления ИБ. Рабочая программа отражает особенности предметных областей каждого из направлений и может иметь различные уровни детализации. Основные разделы представлены в таблице 1.

Таблица 1 – Разделы дисциплины «Основы информационной безопасности»

№	Раздел	Содержание
1	Национальные интересы и угрозы информационной безопасности Российской Федерации	1.1. Предмет основы информационной безопасности. Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. 1.2. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. Угрозы информационному обеспечению государственной политики Российской Федерации. 1.3. Информационные системы. Современное состояние информационной безопасности. Роль и место информационной безопасности. Понятие информационной безопасности. Основные ее составляющие.
2	Угрозы информационной безопасности	2.1. Понятия уязвимости. Понятие угрозы. Основные угрозы информационной безопасности. Классификация угроз. Статистика атак. Основные механизмы защиты. 2.2. Каналы утечки информации. Классификация каналов утечки информации. Каналы утечки информации в типовой информационной системе. Угрозы информационной безопасности. Уязвимости. Каналы утечки информации; 2.3. Атаки инсайдеров. Характеристика и механизмы реализации типовых инсайдерских атак. 2.4. Атаки через Интернет. Характеристика и механизмы реализации типовых удаленных атак. Понятие типовой удаленной атаки. Анализ сетевого трафика. 2.5. Атаки инсайдеров. Характеристика и механизмы реализации типовых инсайдерских атак. 2.6 Атаки через Интернет. Характеристика и механизмы реализации типовых удаленных атак. Понятие типовой удаленной атаки. Анализ сетевого трафика.
3	Законодательный уровень информационной безопасности.	3.1. Законодательный уровень информационной безопасности. Федеральные Законы. 3.2. Руководящие документы Федеральной службы по экспортному и техническому контролю по вопросам информационной безопасности. 3.3. Стандарты и спецификации в области информационной безопасности. Международный стандарт управления информационной безопасностью ISO 17799 . Стандарт ISO/I EC 15408 "Критерии оценки безопасности.
4	Политика информационной безопасности, управление рисками	4.1 Административный уровень информационной безопасности 4.2 Политика информационной безопасности. Структура и основные компоненты политики безопасности 4.3. Управление рисками информационной безопасности. Основные методы оценки рисков.

5	Основные механизмы защиты информации	5.1 Процедурный уровень информационной безопасности 5.2 Основные программные механизмы защиты информации. Идентификация и аутентификация, управление доступом. 5.3 Вирусы и антивирусы. Классификация компьютерных вирусов. Методы обнаружения и удаление компьютерных вирусов. 5.4 Основные технические механизмы защиты информации. Межсетевые экраны. Сканеры безопасности.
6	Управление информационной безопасностью	6.1 Открытые сообщения и их характеристики. Методы шифрования информации. Шифры перестановок и подстановок. Ассиметричное шифрование. 6.2 Электронная подпись. 6.3 Мониторинг и аудит, контроль целостности информации. 6.4 Инциденты информационной безопасности. Методика разбора инцидентов.

Для получения практических навыков в рамках дисциплины «Основы информационной безопасности» должен быть предусмотрен курс практических (лабораторных работ) направленных на развитие умений по применению и конфигурации базовых типов средств защиты информации. Для закрепления и контроля полученных знаний предлагается проводить тестирование и опросы после каждого пройдённого раздела.

В результате успешного освоения дисциплины персонал СЦ сможет:

- повысить свою компетентность в области информационной безопасности;
- более эффективно, в собранных в процессе мониторинга данных, выявлять признаки событий безопасности и прогнозировать сценарии развития инцидента ИБ;
- организовывать и проводить профилактические мероприятия, направленные на предупреждение нарушений ИБ в самом СЦ или снижение рисков их последствий за счет применения защитных механизмов различного типа.

Список литературы

1. Башелханов И.В., Трусов Н.А., Иванус А.И., Колмыкова Е.А., Солодов А.К. Особенности управления комплексной безопасностью в условиях информационного коллапса и сингулярности//Создание единой системы безопасности объектов и территорий государства/ Сб.докладов и статей IX –ой Международной научно-технической конференции «Электронный город-электронная губерния-электронное государство». г.Москва, 18 мая 2016 г. (под ред. Заслуженного изобретателя РФ В.А.Куделькина и д.т.н. Т.Г.Габричидзе.- Самара: Изд-во СГА, 2016.- С.134-146.

2. Башелханов И.В., Трусов Н.А., Колмыкова Е.А. Обеспечение информационной национальной, этнической безопасности и философские междисциплинарные аспекты информационного права//Новые вызовы и угрозы информационной безопасности: правовые проблемы/ Отв.ред.Т.А.Полякова,И.Л.Бачило,В.Б.Наумов. Сб.науч.работ .- М.: Институт государства и права РАН - Изд-во «Канон+» РООИ «Реабилитация», 2016.- С.190-197

3. Елистратов В.С., Пименов П.А. Нейминг: искусство называть.- М.: Издательство «Омега-Л»,2014.-293 с.

4. Иванус А.И., Гармоничный подход к когнитивному управлению инновационной экономикой // «Академия Тринитаризма», М.,Эл № 77-6567, публ.17246, 22.01.2012. http: //www.trinitas.ru/rus/doc/0232/013a/ 02322128.htm. Дата обращения 14.11.2016

5.Назаров В. Стратегическое планирование как важнейший фактор повышения эффективности государственного управления //Власть. 2013.№12. С.4 -11.

6. Никитенко Е.Г. Система распределенных ситуационных центров, работающих по единому регламенту взаимодействия// Пробелы в российском законодательстве. Юридический журнал. 2013. №5. С. 268-270.

7. Прангишвили И.В., Амбарцумян А.А. Основы построения АСУ сложными технологическими процессами.- М.:Энергоатомиздат, 1994.- 304 с.

8. Приказ Роскомнадзора от 21.01.2011 N 27 «О Ситуационном центре Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=629442&rnd=228224.1590515804&from=544576-0#0 (дата обращения 13.11.2016).

9. Пьянков О.В., Романов М.С. Оптимизация процессов принятия решений в ситуационных центрах органов внутренних дел//Вестник Воронежского института МВД.2014.С. №1.

10. Цыбулин А.М., Никишова А.В., Умницы М.Ю. Информационная безопасность для студентов, обучающихся на гуманитарных направлениях//Информационное противодействие угрозам терроризма. 2015. Т. 2. № 25. С. 301-305.

References

1. Bashelkhanov I.V., Trusov N.A., Ivanus A.I., Kolmykova Ye.A., Solodov A.K. Osobennosti upravleniya kompleksnoy bezopasnost'yu v usloviyakh informatsionnogo kollapsa i singulyarnosti//Sozdaniye yedinoy sistemy bezopasnosti ob"yektov i territoriy gosudarstva/ Sb.dokladov i statey IX –oy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «Elektronnyy gorod-elektronnaya guberniya-elektronnoye gosudarstvo». g.Moskva, 18 maya 2016 g. (pod red. Zasluzhennogo izobretatelya RF V.A.Kudel'kina i d.t.n. T.G.Gabrichidze.- Samara: Izd-vo SGA, 2016.- S.134-146.
2. Bashelkhanov I.V., Trusov N.A., Kolmykova Ye.A. Obespecheniye informatsionnoy natsional'noy, etnicheskoy bezopasnosti i filosofskiye mezhdistsiplinarnyye aspekty informatsionnogo prava//Novyye vyzovy i ugrozy informatsionnoy bezopasnosti: pravovyye problemy/ Otv.red.T.A.Polyakova,I.L.Bachilo,V.B.Naumov. Sb.nauch.rabot .- M.: Institut gosudarstva i prava RAN - Izd-vo «Kanon+» ROOI «Reabilitatsiya», 2016.- S.190-197
3. Yelistratov V.S., Pimenov P.A. Neyming: iskusstvo nazyvat'.- M.: Izdatel'stvo «Omega-L»,2014.-293 s.
4. Ivanus A.I., Garmonichnyy podkhod k kognitivnomu upravleniyu innovatsionnoy ekonomikoy // «Akademiya Trinitarizma», M.,El № 77-6567, publ.17246, 22.01.2012. http: //www.trinitas.ru/rus/doc/0232/013a/ 02322128.htm. Data obrashcheniya 14.11.2016
5.Nazarov V. Strategicheskoye planirovaniye kak vazhneyshiy faktor povysheniya effektivnosti gosudarstvennogo upravleniya //Vlast'. 2013.№12. S.4 -11.
6. Nikitenko Ye.G. Sistema raspredelennykh situatsionnykh tsentrov, rabotayushchikh po yedinomu reglamentu vzaimodeystviya// Probely v rossiyskom zakonodatel'stve. Yuridicheskiy zhurnal. 2013. №5. S. 268-270.
7. Prangishvili I.V., Ambartsumyan A.A. Osnovy postroyeniya ASU slozhnymi tekhnologicheskimi protsessami.- M.:Energoatomizdat, 1994.- 304 s.
8. Prikaz Roskomnadzora ot 21.01.2011 N 27 «O Situatsionnom tsentre Federal'noy sluzhby po nadzoru v sfere svyazi, informatsionnykh tekhnologiy i massovykh kommunikatsiy». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=629442&rnd=228224.1590515804&from=544576-0#0 (data obrashcheniya 13.11.2016).
9. P'yankov O.V., Romanov M.S. Optimizatsiya protsessov prinyatiya resheniy v situatsionnykh tsentrakh organov vnutrennikh del//Vestnik Voronezhskogo instituta MVD.2014.S. №1.
10. Tsybulin A.M., Nikishova A.V., Umnitsy M.YU. Informatsionnaya bezopasnost' dlya studentov, obuchayushchikhsya na gumanitarnykh napravleniyakh//Informatsionnoye protivodeystviye ugrozam terrorizma. 2015. T. 2. № 25. S. 301-305.