Кибербезопасность

Типовой учебный план

Кибербезопасность

Типовой учебный план

National Defence
Office of the Commander
Military Personnel Generation
P.O. Box 17000 Station Forces
Kingston, ON K7K 7B4

Défense nationale
Bureau du commandant
Génération du personnel militaire
CP 17000, Succursale Forces
Kingston, ON K7K 7B4

4500-1 (SSO EE)

6 October 2016

Cybersecurity: A Generic Reference Curriculum (RC)

Dear Partners/NATO Members,

It pleases us to share with you the document entitled *Cybersecurity: A Generic Reference Curriculum (RC)*, developed, on behalf of NATO and the Partnership for Peace Consortium (PfPC) of Defense Academies and Security Studies Institutes, by a multinational team of academics and practitioners. This document aims to provide NATO and partner countries with in-depth learning objectives and curriculum support for academic courses broadly related to Cybersecurity.

The Cybersecurity Reference Curriculum consists of four themes: i) Cyberspace and the Fundamentals of Cybersecurity, ii) Risk Vectors, iii) International Cybersecurity Organizations, Policies and Standards and iv) Cybersecurity Management in the National Context. The four themes and associated blocks have been carefully chosen to encompass the broadest spectrum of Cybersecurity issues and topics, and to provide the most pertinent level of education.

This document is best understood as a resource to NATO and partner countries looking to develop and gain greater appreciation of the spectrum of issues, national and international, entangled in the practices of cybersecurity. It is presented in the hope that it will be noted by NATO in due time through the appropriate committees. The next envisioned step will be to work with partner defense education establishments in

4500-1 (OSEM PED)

Le octobre 2016

Programme de reference (PR) générique de la Cybersécurité

Chers partenaires/membres de l'OTAN,

Il nous fait grand plaisir de partager avec vous le document intitulé *Programme de référence (PR) générique de la Cybersécurité* développé par une équipe multinationale d'universitaires et de praticiens au nom de l'OTAN et du Groupement d'institutions d'études de défense et de sécurité du Partenariat pour la paix (PPP). L'objectif de ce document est d'offrir à l'OTAN et aux pays partenaires un appui dans le développement d'objectifs d'apprentissage et de contenu pour les cours liés aux études de la Cybersécurité.

Le programme de référence de la Cybersécurité se compose de quatres étapes : i) cyberespace et les principes fondamentaux de la cybersécurité, ii) vecteurs de risque, iii) organisations internationales cybersécurité , politiques et normes, et iv) la gestion de la cybersécurité dans le contexte national. Les quatre étapes et les thèmes associés ont été choisis avec soin pour englober la plus grande gamme possible de questions et de thématiques de cybersécurité et fournir le niveau le plus pertinent d'éducation.

Ce document sert de ressource à l'OTAN et ses partenaires cherchant à développer une image plus complète de l'ensemble des questions nationales et internationales, empêtré dans les pratiques de la cybersécurité. Il est présenté dans l'espoir qu'il sera entériné par l'OTAN en temps opportun par le biais de comités appropriés. La prochaine étape consistera à collaborer avec les institutions partenaires d'éducation militaire lors de l'adoption et de la

their adoption and implementation of all or parts of this curriculum, guided by their Individual Partnership Action Plan (IPAP).

Only through dialogue and exchange of ideas can this document enhance the professional development and interoperability of alliance and partner military members. I invite your delegation personnel to distribute this document widely in your respective countries.

If you have any questions regarding this curriculum, please have your delegation personnel contact Mr. Sean Costigan, George C. Marshall European Center for Security Studies at sean.costigan@pfp-consortium.org or Dr. Michael Hennessy, Professor of History and War Studies, Royal Military College of Canada at hennessy-m@rmc.ca

Best wishes,

Le commandant,
Major-général

J.G.E. Tremblay
Major-General
Commander

mise en œuvre de ce programme, en tout ou en partie, selon leur plan d'action individuel pour le partenariat (IPAP).

C'est uniquement à travers le dialogue et l'échange d'expériences que ce document contribuera positivement à l'interopérabilité des sous-officiers de l'alliance et des pays partenaires, et à leur éducation militaire. Nous invitons le personnel de votre délégation à le diffuser à grande échelle dans vos pays respectifs.

Pour de plus amples renseignements sur le programme, le personnel de votre délégation peut communiquer avec M. Sean Costigan, Centre George C. Marshall European Center for Security Studies au sean.costigan@pfp-consortium.org ou M. Michael Hennessy, Professeur d'histoire et d'études sur la conduite de la guerre, Collège militaire royal du Canada au hennessy-m@rmc.ca

Nous vous prions d'agréer nos salutations les plus distinguées.

Министерство национальной обороны
Начальник Главного управления формирования кадров МНО Канады
P.O. Box 17000 Station Forces
Kingston, ON K7K 784

4500-1 (SSO EE)

6 октября 2016

Кибербезопасность: Типовой учебный план (УП)

Дорогие партнеры/члены НАТО,
Мы с удовольствием хотим поделиться с вами документом под названием «Кибербезопасность: типовой учебный план» (УП), разработанным по поручению НАТО и Консорциума программы Партнерства мира (PFPC) военных академий и исследовательских институтов, многонациональной командой ученых и практиков. Этот документ призван представить НАТО и странам-партнерам цели углубленного обучения и поддержки учебных программ курсов теоретической подготовки, в широком смысле связанных с кибербезопасностью.
«Кибербезопасность: типовой учебный план» состоит из четырех разделов: i) Киберпространство и основы кибербезопасности, ii) Векторы риска, iii) Международные организации в сфере кибербезопасности, политики и стандартов, и iv) Управление кибербезопасностью в национальном контексте. Четыре раздела и сопутствующие материалы были тщательно подобраны с целью охвата предельно широкого спектра вопросов и предметов кибербезопасности, и обеспечения наиболее уместного уровня образования.
На данный документ лучше смотреть как на ресурс для НАТО и стран-партнеров, стремящихся наилучшим образом понять разобраться в широком диапазоне вопросов - внутренних и международных, - заложенных в практику обеспечения кибербезопасности.

Документ представлен в надежде на то, что соответствующие комитеты НАТО отметят его целесообразность. Мы представляем, что следующим шагом будет принятие и внедрение всего или частичного учебного плана партнерскими военными академиями и училищами, в соответствии с их Индивидуальным планом партнерства с НАТО (IPAP). Только путем диалога и обмена идеями, этот документ сможет помочь в повышении профессиональной квалификации и оперативной совместимости Альянса и военных партнеров. Я призываю членов ваших делегаций дать данному документу широкое распространение в своих странах.
Если у вас возникнут какие-либо вопросы в отношении Учебного плана, пусть члены вашей делегации свяжутся с г-ном Шоном Костиганом в Европейском центре по изучению вопросов безопасности им. Джорджа К. Маршалла по адресу: sean.costigan@pfp-consortium.org или с д-ром Майклом Хеннесси, профессором истории и военных исследований Королевского военного колледжа Канады по адресу: hennessy-m@rmc.ca

С наилучшими пожеланиями,

Начальник ГУФК МНО

Канады генерал-майор Эрик Трамбле

NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
HEADQUARTERS SUPREME ALLIED COMMANDER TRANSFORMATION
7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA, 23551-2490

5000/TSC TTX 0310/TT-161157/Ser: NU0766(INV)

TO: See Distribution

SUBJECT: Endorsement of the PfPC Emerging Security Challenges Working Group Cybersecurity Reference Curriculum as a NATO Educational Reference Document

DATE: 27 September 2016

1. In an effort to satisfy specific partner education and training needs, the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group (ESCWG) has developed a Cybersecurity Reference Curriculum. The efforts, professionalism and dedication of those who contributed to the development of the curriculum is commendable.

2. The Cybersecurity Reference Curriculum is found compatible with NATO Education and Training on Cyber Defence and I am convinced that it can serve as a reference for partner countries in the design and development of course models and programmes for professional Cybersecurity military education. It will also serve as an enhancement of military interoperability between NATO and its partners and strengthen the collaboration on a responsive education and training system.

3. It is my pleasure to support the PfPC Emerging Security Challenges Working Group through publishing this Cybersecurity Reference Curriculum as a NATO document. I encourage all respective instructional designers of partner countries involved in the development of related learning opportunities to make full use of this guide.

4. Should there be any questions, please contact Mr. Salih Cem Kumsal, NATO Cyber Defence Education and Training Discipline POC at +1 (757) 747-3386, NCN 555-3386, or email cem.kumsal@act.nato.int.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION:

for
Stefano Vito Salamida
Major General, ITA AF
DCOS Joint Force Trainer

Североатлантический союз (НАТО)

Штаб-квартира Верховного главнокомандующего
ОВС НАТО по трансформации

7857 Blandy Road, Suite 100
Norfolk, Virginia 23551-2490

Тема: Свидетельство в пользу использования «Кибербезопасность: типовой учебный план», разработанного Рабочей группой по формирующимся вызовам в сфере безопасности Консорциума «Партнерство ради мира», в качестве учебного справочного материала.

Дата: 27 сентября 2016 г.

1. В стремлении удовлетворить конкретные нужды в сфере обучения и подготовки кадров, Рабочая группа по новым вызовам в сфере безопасности Консорциума «Партнерство ради мира» (РГНВБ) разработала Типовой учебный план по кибербезопасности. Достойны похвалы приложенные усилия, приверженность делу и профессионализм всех тех, кто внес вклад в разработку Учебного плана.

2. «Кибербезопасность: типовой учебный план» соответствует целям НАТО по образованию и подготовке в области кибероборонь и я убежден, что он может служить справочником для стран-партнеров в создании и разработке курсовых моделей и программ для профессионального военного образования в области кибероборонь. Он также послужит расширению оперативной совместимости между НАТО и странами-партнерами и укрепит сотрудничество в развитии оперативной системы образования и подготовки.

3. Я с удовольствием выражаю свою поддержку Рабочей группой по новым вызовам в сфере безопасности посредством публикации справочника «Кибербезопасность: типовой учебный план» в качестве документа НАТО. Я призываю всех соответствующих методистов педагогического проектирования стран-партнеров, участвующих в разработке учебных программ, имеющих отношение к кибербезопасности, в полной мере использовать данное руководство.

4. В случае возникновения каких-либо вопросов, прошу вас связаться с г-ном Салихом Джем Кумсалом – контактным лицом Программы образования и обучения в области кибербезопасности НАТО – по телефону +1 (757) 747-3386, либо NCN 555-3386. Вы также можете отправить ему сообщение по электронной почте: cem.kumsal@act.nato.int

ЗА ВЕРХОВНОГО ГЛАВНОКОМАНДУЮЩЕГО НАТО ПО ТРАНСФОРМАЦИИ

(подпись) Стефано Вито Саламида

Генерал-майор, ВВС Италии

Зам. Начальника штаба Учебного центра объединенных сил НАТО

О типовом учебном плане

Настоящий документ является результатом работы многонациональной группы работавших на добровольной основе ученых и исследователей из 17 стран, связанных с Рабочей группой по новым вызовам безопасности (РГНВБ) Консорциума ПРМ. Нашей целью была разработка гибкого и большей частью комплексного подхода к вопросу кибербезопасности.

Цель настоящего документа – обеспечить широкое рассмотрение кибербезопасности, при сохранении достаточной глубины, с тем чтобы нетехнические специалисты получили более полное представление о технологических аспектах, и чтобы технические специалисты в более полной мере осознали последствия для политики безопасности на национальном и международном уровнях и для оборонной политики. Мы предлагаем логичную разбивку темы на конкретные категории, предлагаем уровень знаний, который могут приобрести различные аудитории и указываем полезные ключевые ссылки, с тем чтобы каждое принимающее государство могло адаптировать эти рамки к своим нуждам и к особенностям целевого контингента обучаемых.

Мы особенно благодарны Консорциуму военных академий и институтов, занимающихся исследованием проблем безопасности по программе «Партнерство ради мира», его руководителю Рафаэлю Перлу, председателям РГНВБ, д-ру Детлефу Пулю (НАТО) и д-ру Густаву Линдстрому (ЖЦПБ), а также выражаем признательность за поддержку со стороны Рабочей группы по Программе углубления военного образования и Рабочей группы по образованию Консорциума ПРМ под руководством д-ра Эла Столберга, д-ра Жана д'Андурайна и д-ра Дэвида Эмелифеонву. Кроме того, руководство нескольких государств-партнеров, включая Армению, Грузию и Молдову, помогли в реализации этих усилий посредством непосредственной и ощутимой поддержки. И наконец, что немаловажно, огромную благодарность заслуживают все те, кто работал на добровольной основе. Когда мы спросили их, готовы ли они участвовать в двухлетней работе, которая приведет их в глубины образования в области кибербезопасности, никто из них не отступил. Мы, в частности, хотели бы поблагодарить Скотта Найта, Диноса Керигана-Кайру, Филипа Ларка, Криса Палларис, Даниэля Педера Багге, Джиджи Романа, Наталью Спину, Тодора Тагарева, Рональда Тейлора и Джозефа Вана. Без них просто невозможно было бы создать этот документ.

Шон Костиган и Майкл Хеннесси

Мы выражаем особую благодарность настоящим профессионалам - сотрудникам отдела переводов Центра им. Джорджа К. Маршалла и в особенности Александру Гурману и Джин Крамер, без которых было бы невозможно осуществить данный перевод.

I. ЦЕЛЬ НАСТОЯЩЕГО ДОКУМЕНТА

Стремительные и неумолимые изменения и вызовы в области кибербезопасности[1] стали движущей силой, которая побудила РГНВБ сделать запрос на разработку настоящего учебного плана, с учетом того, что НАТО уделяет особое внимание повышение информированности, готовности и устойчивости в области кибербезопасности.

Заголовки новостей содержат множество сообщений о взломах коммерческих структур, утечке данных, электронном мошенничестве, нарушениях функционирования государственных структур или критически важных объектов инфраструктуры, кражах интеллектуальной собственности, утечке информации, связанной с национальной безопасностью, и потенциальном киберуничтожении. Та сфера, которая когда-то считалась электронной войной или информационной войной, и в которой преобладали специалисты по сетевой безопасности, сегодня преобразовывается в более широкую сферу, именуемую «кибербезопасность».

Поскольку это новая проблема, в рамках которой сохраняются разногласия в отношении основных терминов, РГНВБ стремится внести ясность и обеспечить унификацию посредством разработки настоящего типового учебного плана. Мы утвердили согласованное написание термина «кибербезопасность» (“cybersecurity”) в одно слово по всему документу и используем термин «кибер» (“cyber”) в качестве определения или для разъяснения направленности.

При составлении настоящего документа мы опросили институты, входящие в Консорциум ПРМ, и другие военные учебные заведения и сделали обзор программ военной подготовки в государствах-партнерах НАТО и Консорциума ПРМ, чтобы установить, что входит в их программы обучения. Мы стремились выявить пробелы и общие подходы, которые не ограничиваются традиционными рамками правительственных и военных структур. Наибольшим пробелом, который мы констатировали, было отсутствие достаточного понимания технологии кибербезопасности и практики смягчения угрозы и риска среди руководителей в области политики национальной безопасности и обороны. Аналогичный пробел в понимании рамок национальной политики был выявлен среди технических специалистов.

Настоящий типовой учебный план обеспечивает согласованную отправную точку для разработки или совершенствования обучения по вопросам кибербезопасности для старших офицеров, государственных служащих и военного и гражданского персонал среднего звена. Цель настоящего документа, как и других типовых учебных планов, разработанных Консорциумом ПРМ, является консервативной. Это не универсальное описание курса, которому все должны следовать. Он не является исчерпывающим по содержанию, деталям или подходам к теме. Тем не менее, мы считаем, что он обеспечивает полезный эвристический подход к различным областям и включает всеобъемлющее введение в круг вопросов, связанных с практикой кибербезопасности. Тем, чьи технические знания ограничены, уровень сложности введения покажется приемлемым; кроме того, они смогут лучше понять, где и зачем требуются глубокие технические знания. Для тех, кто имеет технический опыт, данный материал будет полезным обзором областей, с которыми они знакомы, и введением в более широкие вопросы международной, национальной и правовой политики и практики. Мы надеемся, что каждый найдет в нем что-то полезное.

Желающие использовать этот документ в качестве подхода к кибербезопасности должны проанализировать свои конкретные и уникальные национальные виды практики и требования, чтобы приспособить его к своим потребностям. В этом документе содержатся рекомендации в определении областей, которые требуют внимания и рекомендует основные источники и подходы.

II. КИБЕРБЕЗОПАСНОСТЬ И РИСКИ

Наиболее часто меры безопасности обуславливаются уровнем угроз и рисков. Оба понятия рассматриваются достаточно подробно. Однако, говоря простым языком, киберпространство полно угроз, но меры по смягчению угроз должны обуславливаться уровнем риска. Международная организация по стандартизации (ИСО) определяет риск как «влияние неопределенности на цели» (влияние может быть положительным или отрицательным отклонением от ожидаемого). Поскольку меры, принимаемые для обеспечения безопасности чего-либо должны быть пропорциональны ценности того, чья безопасность обеспечивается, существуют различные уровни безопасности в зависимости от уровня ценности и риска. Обеспечение безопасности киберпространства, следовательно, влечет за собой ряд соображений для уменьшения рисков и угроз, поощряя доступность и открытость для всех различных видов взаимосвязанных сетей и устройств. Установление необходимого баланса между доступом, применимостью и безопасностью является основной задачей. Настоящий учебный план рассматривает подходы к оценке и идентификации угроз и рисков, и к смягчению их последствий, как на техническом уровне, так и на

[1] В принципе, мы используем определение, разработанное для Министерства внутренней безопасности США: «Кибербезопасность – это деятельность или процесс, способность, возможность или состояние, при которых системы информации и связи и информация, содержащаяся в них, защищены и/или охраняются от вреда, несанкционированного использования, модификации или эксплуатации».

уровне ведомственной и государственной политики, путем изучения рекомендуемого передового опыта и в сравнении с опубликованной политикой отдельных государств или организаций.

III. СТРУКТУРА НАСТОЯЩЕГО УЧЕБНОГО ПЛАНА

Как заявлялось в предыдущих учебных планах, план обучения представляет собой конкретную учебную программу или, возможно, ряд курсов, которые в совокупности описывают материалы и методы преподавания, обучения и оценки, соответствующих данной программе обучения. Поэтому получаемый учебный план – это «дорожная карта» того, что может ожидать обучаемых. Как и любая карта, она создана на уровне абстракции и может не показывать все маршруты или детали; однако, он описывает то, что обучаемый должен увидеть.

Как правило, типовой учебный план приводит к созданию иерархической структуры с множеством подтем и вопросов, вписанных в широкие рамки[2]. Эти многочисленные иерархические составляющие связаны с более широкими целями программы обучения. Учитывая взаимосвязанность предметов и вопросов, содержащихся в нашем учебном плане по кибербезопасности, мы не рекомендуем разбивать учебный план на три этапа подготовки сотрудников. Более подробно об этом ниже, когда мы будем рассматривать, как использовать этот учебный план.

В соответствии со структурами, принятыми в других типовых учебных планах Консорциума ПРМ, данный документ представлен четырьмя темами, каждая из которых разделена на блоки, которые, естественно, могут быть далее подразделены. Эти подразделения обозначены как темы (Т) и блоки (В), что отражено в оглавлении (см. ниже).

Данный учебный план включает следующие четыре темы:

Тема 1: Киберпространство и основы кибербезопасности

Тема 2: Векторы риска

Тема 3: Международные организации по кибербезопасности, принципы и стандарты

Тема 4: Менеджмент кибербезопасности в национальном контексте

Все темы подробно описаны в других частях настоящего документа, при этом каждая тема содержит широкий круг конкретных областей и вопросов, подлежащих рассмотрению.

Каждая тема включает несколько отдельных дисциплин. Каждая дисциплина изучается в рамках базовых блоков, каждый из которых может быть разбит на отдельные учебные модули, такие как лекции, презентации, демонстрации, учебно-ознакомительные поездки, упражнения по конкретным сценариям или аналогичные виды деятельности. В большинстве случаев, поскольку настоящий типовой учебный план будет требовать местной адаптации, мы не предлагаем отдельных модулей и лекций, потому что такой уровень детализации зависит от индивидуальных потребностей. Вместе различные блоки положены в основу каждой темы. Они рекомендуют, какие должны быть достигнуты цели и результаты; которые в свою очередь связаны с более широкими целями тем.

Блоки могут преподаваться в целом, комбинированно или в разделении на отдельные модули. В настоящем плане нет рекомендаций о том, каким именно образом организовывать обучение по конкретным блокам, но как в блоках, так и в модулях обучение дисциплинам может осуществляться в виде лекций, презентаций, заданий на основе активного участия, учебно-ознакомительных поездок, демонстраций или участия в упражнениях по конкретным сценариям.

IV. ПРИМЕНЕНИЕ УЧЕБНОГО ПЛАНА

Настоящий учебный план делает ряд неявных предположений.

Во-первых, все материалы, определенные в настоящем документе, не являются конфиденциальными. Лица, принимающие настоящие рамки, могут пожелать рассмотреть конфиденциальные материалы, если возникнет такая необходимость.

Во-вторых, предполагается, что институты, принимающие настоящий типовой учебный план, уделят соответствующее время и ресурсы тому, чтобы совместно с группой экспертов определить национальную политику и процедуры на уровне детализации, необходимом для целевой аудитории. Механически приобретенные технические знания могут оказаться необходимыми, но в данном случае целью является более широкое понимание вызовов в области кибербезопасности по всему спектру вопросов.

При адаптации настоящего учебного плана к использованию на местах возможно его поступательное и последовательное выполнение на всех этапах карьеры, но на всех уровнях необходимо следовать комплексному

[2] См. предыдущие типовые учебные планы, в которых описаны истоки и применимость данной концепции.

плану. Однако широкая цель настоящего типового учебного плана является скорее стратегически-оперативной, чем тактической. При разработке конкретных курсов на основе настоящего типового учебного плана рекомендуется, чтобы составители курса принимали во внимание имеющиеся время и ресурсы, уровень образования обучаемых и функции, которые, как ожидается, должны будут выполнять, независимо от их званий.

В-третьих, в плане нет блока, посвященного кибервойнам, киберконфликтам или социальным сетям, в качестве канала для пропаганды и дезинформации. Комитет по составлению курсов решил оставить эти целенаправленные вопросы для последующей разработки.

И наконец, мы подчеркиваем, что настоящий типовой учебный план не является единой или предлагаемой структурой курса. План, скорее, лучше использовать в качестве ключевого справочного документа, представляющего широкий обзор вопросов и тем по всему спектру кибербезопасности. Он может служить руководством, позволяющим техническим специалистам понять, на что в широком спектре вопросов обращено их особое внимание. Аналогичным образом, он может служить руководством для вводных курсов, предназначенных для высокопоставленных лиц, отвечающих за формирование политики в области национальной безопасности, с тем чтобы они могли лучше понимать национальную политику и помещать ее в определенный контекст на основе технических знаний. Тремя элементами, вызывающими особую озабоченность при создании единого курса на основе настоящего плана, будут: цели или задачи курса; предполагаемые обучаемые, особенно уровень их технических знаний и характер их работы; и имеющееся в наличии время. Эти три элемента должны определять уровень технической детализации и характер учебных упражнений (лекции, примеры, учебно-ознакомительные поездки, демонстрации, военные игры и т.д.).

V. ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ

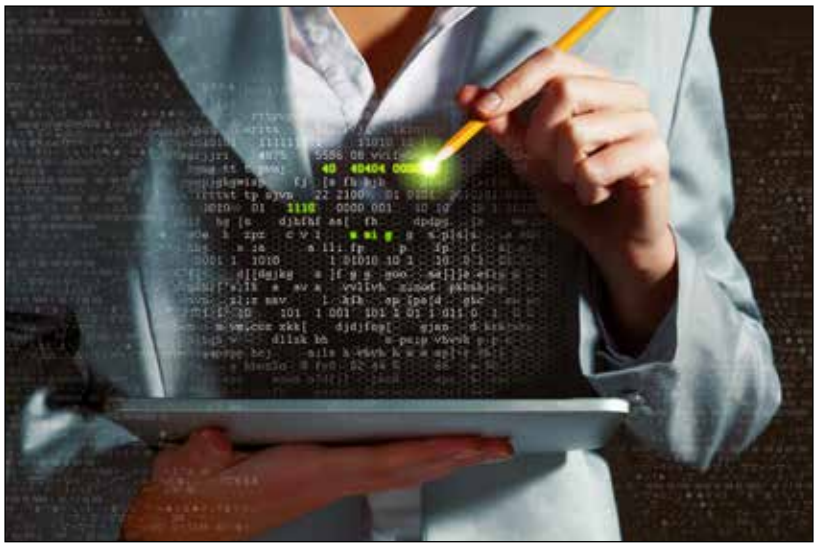
Объем общей и технической литературы по кибербезопасности быстро растет. Составителям курсов рекомендуется создавать собственные перечни ключевых источников; тем не менее, мы включили, широкий круг источников, отражающих многие различные национальные и международные точки зрения, имеющие отношение к темам, сформулированным для настоящего типового учебного, и, при наличии возможности, мы предоставили ссылки на действующие Интернет-ресурсы. Помимо многочисленных источников, перечисленных в настоящем документе, сайт НАТО предлагает множество современных статей и информации по вопросам, представляющим интерес для сообщества НАТО. Среди источников, перечисленных по адресу: www.natolibguides.info/cybersecurity:

- Статьи/видеоматериалы из «Вестника НАТО» о кибернападениях, а также выпуск от июня 2013 г. «Киберпространство: хорошее, плохое и свободное от вирусов» (содержит видеоматериалы, фотоматериалы, хронику событий, инфографику и т.д.).
- Статья NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow by Healey and van Bochoven (февраль 2012), предлагает хороший обзор киберпотенциала НАТО.
- Доклад On Cyberwarfare (2012) by Fred Schreier, содержит глоссарий и очень хорошую подборку тематической литературы (официальные документы, НАТО, ОЭСР, по странам, информационная война, кибербезопасность, книги).
- The Cyber Special Edition of *Strategic Studies Quarterly* 6, no. 3 (о 2012).
- The Cybersecurity: Shared Risks, Shared Responsibilities edition of *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012).
- Статья Cyberspace Is Not a Warfighting Domain (2012) by Martin Libicki.
- Таллинское руководство по международному праву, применимому к кибервойне (2012).
- 300-страничное руководство, составленное группой из 20 исследователей по приглашению Центра передового опыта НАТО по совместной защите от киберугроз в Таллине (Эстония).
- Последующий проект «Таллин 2.0» в развитие *Таллинского руководства по международному праву, применимому к кибервойне* предназначен для расширения охвата первоначального *Таллинского руководства*. Результатом проекта «Таллин 2.0» будет второе издание *Таллинского руководства издательством* Cambridge University Press в 2016 г. (источник: Центр передового опыта НАТО по совместной защите от киберугроз).
- The National Cyber Security Framework Manual (2012), Центр передового опыта НАТО по совместной защите от киберугроз.
- Электронный учебный курс Центра передового опыта НАТО по совместной защите от киберугроз Cyber Defence Awareness (предоставляется бесплатный доступ, но требуется регистрация).

- The Cyber Conflict Bibliography by the Jacob Burns Law Library, George Washington University Law School.
- Брифинг Cyber defence in the EU: Preparing for cyber warfare? (31 October 2014) by the European Parliamentary Research Service.
- The Tallinn Paper no. 8, published in April 2015: "The Role of Offensive Cyber Operations in NATO's Collective Defence."

Среди других полезных источников:

- Business Continuity Institute, *Good Practices Guidelines 2013, Global Edition: A Guide to Global Good Practice in Business Continuity* (England, 2013). http://www.thebci.org/index.php/resources/the-good-practice-guidelines
- Gustav Lindstrom, "Meeting the Cyber Security Challenge," *GCSP Geneva Papers—Research Series* no. 7 (June 2012).
- International Auditing and Assurance Standards Board, ISAE 3402 Standard for Reporting on Controls at Service Organizations.
- ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4.
- ITU-D Study Group 1, Final Report, *Question 22-1/1: Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity*, 5th Study Period 2010¬–2014. See http://www.itu.int/ITU-D/study_groups or http://www.itu.int/pub/D-STG-SG01.22.1-2014.
- J. Lewis and K. Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, Washington, DC, 2011.
- National Initiative for Cybersecurity Careers and Studies http://niccs.us-cert.gov/glossary
- Neil Robinson, Luke Gribbon, Veronika Horvath and Kate Robertson, *Cybersecurity Threat Characterisation: A Rapid Comparative Analysis* (Santa Monica, CA: Rand Corporation, 2013), prepared for the Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, Stockholm.
- NIST Special Publication 800-82: Guide to Industrial Control Systems Security, June 2011.
- Ron Deibert and Rafal Rohozinski, *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, joint report by the Information Warfare Monitor and Shadowserver Foundation, JR-03-2010, April 6, 2010. http://shadows-in-the-cloud.net
- U.S. Department of Defense, The DoD Cyber Strategy, April 2015, Washington, DC.
- World Economic Forum, *Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats*. Industry Agenda item (in collaboration with Deloitte), Ref. 301214, 2015.



ОГЛАВЛЕНИЕ

Тема 1: Киберпространство и основы кибербезопасности

Цель

Цель данной темы – заложить основу знаний для всего последующего обучения путем определения структурных компонентов киберпространства[3], его основной архитектуры и основ кибербезопасности. Идентификация рисков и управление ими – главная общая задача, связывающая отдельные темы и дисциплины, рассматриваемые в настоящем учебном плане.

Описание

Вызовы, связанные с киберпространством и кибербезопасностью, требуют не только простого переименования государственных организаций, ответственных за безопасность в области информационных технологий или за безопасность в области коммуникаций. Повсеместность современных компьютерных систем и способность осуществлять связь или взаимодействовать с помощью различных средств, от мобильных устройств до носимых компьютеров, создают для государственных и негосударственных субъектов ряд неотъемлемых уязвимостей и возможные векторы атак. Использование этих уязвимостей может привести к широким последствиям для национальной безопасности посредством таких намеренных действий, как шпионаж, снижение эффективности объектов командования и управления, кража интеллектуальной собственности и чувствительной информации личного характера, нарушение предоставление существенных услуг и функционирования критически важной инфраструктуры или нанесение ущербы экономике и промышленности.

В ходе изучения пяти блоков данной темы обучаемые познакомятся с базовой структурой киберпространства и с основанным на рисках подходе к кибербезопасности. В T1-B1 «Кибербезопасность и киберпространство – введение» рассматриваются возникновение и общая форма киберпространства, а также вводится концепция кибербезопасности. В T1-B2 «Информационная безопасность и риски», рассматриваются основы методологии анализа рисков в области информационной безопасности и изучается основанный на угрозах подход к оценке. В T1-B3 «Структура информационного пространства: опорная сеть Интернета и сетевая инфраструктура государств» изучается функционирование и архитектура глобального Интернета, а также управление им. В T1-B4 «Протоколы и платформы» представлены стандарты сетевых и информационных технологий с тем, чтобы изучить основы проектирования и эксплуатации сетей. И наконец, в T1-B5 «Архитектура сетевой безопасности и управление процессом обеспечения безопасности» представлены основы архитектуры безопасности, опирающейся на анализ угроз, рисков и уязвимостей. Анализ рисков должен направлять и служить основой для разработки киберархитектуры и киберстратегий, чтобы ограничивать известные и неизвестные уязвимости и угрозы на организационном и национальном уровнях. Соответственно, обучаемые знакомятся с основами методологии анализа киберрисков и их управлением, используемых для разработки архитектуры и стратегий систем, направленных на снижение таких рисков.

Результаты обучения

Обучаемые смогут:

- объяснить, что имеется в виду под киберпространством и кибербезопасностью;
- обозначить некоторые основные уязвимости развитых государств перед киберугрозами, такими как сбор экономической разведывательной информации в интересах государства, профилирование отдельных лиц и организаций, кража данных, порча баз данных или захват промышленных систем управления или систем управления процессами (например, SCADA);
- описать основную топологию киберпространства, включая его физические структуры, а также то, как оно управляется протоколами и процедурами; и
- сформулировать основные принципы надлежащей архитектуры безопасности.

Рекомендуемые учебные и справочные материалы

Lukasz Godon, “Structure of the Internet.” http://internethistory.eu/index.php/structure-of-the-internet/

Dave Clemente, “Cyber Security and Global Interdependence: What is Critical?,” Chatham House Paper, *The Royal Institute of International Affairs*, ISBN 978-1-86203-278-1, February 2013.

Communications Security Establishment Canada (CSEC), *Harmonized Threat and Risk Assessment (TRA) Methodology*, 23 October 2007.

D.P. Cornish, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*, European Parliament Directorate-General for External Policies of the Union, Directorate B—Policy Department, February 2009, EP/EXPO/B/AFET/FWC/2006-10/Lot4/15 PE 406.997. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

[3] Здесь под киберпространством подразумевается электронный мир, созданный взаимосвязанными сетями информационных технологий и информацией об этих сетях. Основано на Canada’s Cyber Security Strategy, 2014.

Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem—Full Report*, ENISA, April 2011. http://www.enisa.europa.eu

R. Tehan, *Cybersecurity: Authoritative Reports and Resources, by Topic*, Congressional Research Service, CRS Report 7-7500 R42507, 15 April 2015. http://www.crs.gov

The White House, *Cyberspace Policy Review*, 2009. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Ethan Zuckerman and Andrew McLaughlin, "Introduction to Internet Architecture and Institutions." https://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html

Семинар группы составителей Учебного руководства по кибербезопасности в Кишиневе.

Блок T1-B1: Кибербезопасность и киберпространство – введение

Описание

Киберпространство состоит из различных подключенных к сети компьютерных систем и интегрированных телекоммуникационных систем. Оно стало одной из характерных особенностей современного общества, обеспечивающей и расширяющей быструю коммуникацию, функционирование распределенных систем командования и управления, хранение и передачу больших массивов данных и функционирование сильно распределенных систем. Сегодня все это воспринимается обществом как должное и стало необходимым для бизнеса, повседневной жизни и предоставления услуг. Такая повсеместность киберпространства и зависимость от него наблюдается даже в военной сфере, где связь, командование и управление, элементы ведения разведки и нанесения высокоточных ударов полагаются на многочисленные «киберсистемы» и связанные с ними коммуникационные системы. Повсеместность этих взаимосвязанных систем привела к некоторой зависимости и уязвимости отдельных лиц, секторов промышленности и правительств, которые трудно прогнозировать, управлять, ослаблять, предотвращать и которыми трудно управлять. Некоторые страны рассматривают такие уязвимость и зависимость как новые проблемы в области национальной безопасности и национальной обороны и ставят задачу существующим структурам своих сил безопасности реагировать на них, в то время как другие страны создают совершенно новые организации, чья задача – управление или координация национальных стратегий в области кибербезопасности. Кибербезопасность стала важным междисциплинарным вопросом, требующим реакции лиц, частных предприятий, неправительственных организаций, «всего правительства» и ряда международных учреждений и органов.

Цель данного блока – познакомить обучаемых с информационно-коммуникационными технологиями в этой области, наглядно показав их повсеместность и присущую нам зависимость от таких систем. Цель – обеспечить широкое понимание социологических, технический и культурных аспектов современных информационных технологий, их множественной роли и влияния киберпространства как условной среды на современную жизнь, управление государством и глобальные коммуникации. Данный блок служит в качестве базовой информации для изучающих вопросы национальной безопасности, чтобы они могли иметь твердое понимание топологии и структурных компонентов киберпространства и кибербезопасности.

Для обеспечения четкости определений мы полагались на определение киберпространства, которое дает Национальный институт стандартов и технологий США: «взаимозависимая сеть инфраструктур информационных технологий, включая Интернет, телекоммуникационных сетей, компьютерных систем, встроенных процессоров и контроллеров…» Кибербезопасность определяется как «деятельность или процесс, способность, возможность или состояние, при которых системы информации и связи и информация, содержащаяся в них, защищены и/или охраняются от вреда, несанкционированного использования, модификации или эксплуатации». На этом базовом определении основана вся информация, включенная нами в настоящий документ.

Результаты обучения

Обучаемые смогут продемонстрировать соответствующий уровень понимания:

- важности информационно-коммуникационных технологий и того, как они изменяют структуру современных обществ;
- нюансов кибербезопасности в различных национальных и культурных контекстах с уделением особого внимания национальным подходам и стратегиям;
- ключевых проблем в области информационно-коммуникационных технологий, ключевых провайдеров, ключевых источников политики, ключевых заинтересованных сторон, юридической ответственности и функциональных обязанностей;
- положительного и отрицательного воздействия киберпространства на общество;
- широкой информированности об угрозах и рисках для эффективного и безопасного функционирования киберпространства;
- того, как осуществляется управление Интернетом, его функционирование и поддержание посредством сети государственных, частных и некоммерческих организаций;
- уникального национального контекста в разработке политики в отношении Интернета и в его управлении на местах;
- роли стандартов и протоколов в проектировании Интернета; и
- военно-политических требований, связанных с киберпространством и управлением Интернетом.

Вопросы и подходы, которые в перспективе могут быть включены в модули

Глубина изучения будет зависеть от аудитории и имеющегося времени; однако модули, посвященные национальной Интернет- и телекоммуникационной инфраструктуре, ключевым провайдерам услуг и современному разделению обязанностей для политики и широкой практике в области безопасности в национальном правительстве и организации по обороне могут рассматриваться отдельно для обеспечения четкости и уделения особого внимания.

Методика обучения/оценка результатов

Методы преподавания могут включать лекции профильных экспертов, семинары, демонстрации, упражнения и моделирование в аудиториях.

Обучаемые оцениваются на основе их участия и обсуждения в ходе упражнений и дискуссий, после которых следует тест на проверку знаний, приобретенных в ходе курса.

Учебные и справочные материалы

Профильные эксперты будут сотрудничать с принимающей страной в целях отбора соответствующих ключевых материалов для чтения на основе запланированной целенаправленности курса и установленных сроков.

Избранные учебные и справочные материалы могут включать:

"'G.I.G.O. Garbage In, Garbage Out' (1969) Computer History—A British View," YouTube, accessed 25 April 2015. http://youtu.be/R2ocgaq6d5s

James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Mass.: Harvard University Press), 1986.

Vinton G. Cerf (Chair) et al., *ICANN's Role in the Internet Governance Ecosystem*, report of the ICANN Strategy Panel, 20 February 2014.

Paul E. Ceruzzi, *A History of Modern Computing*, 2nd ed. (Cambridge, Mass.: MIT Press), 2003.

Paul Hoffman, ed., "The TAO of IETF: A Novice's Guide to the Internet Engineering Task Force," Internet Engineering Task Force, 2015.

Barry Leiner, Vinton Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts and Stephen Wolff, "Brief History of the Internet," accessed 25 April 2015. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Marie-Laure Ryan, Lori Emerson and Benjamin J. Robertson, eds., *The Johns Hopkins Guide to Digital Media* (Baltimore: Johns Hopkins University Press), 2014.

Lance Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation," *Western Journal of Communication* 63, no. 3 (1999): 382–412. doi: 10.1080/10570319909374648

The White House, *International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World* (Washington, DC: Executive Office of the President of the United States, National Security Council), 2011.

Jie Wang, A. Zachary Kissel, "Introduction to Network Security: Theory and Practice", Singapore: Wiley, 2015. ISBN 9781118939505. UIN: BLL01017585410.

EU ENISA, "Cybersecurity as an Economic Enabler" Heraklion, Crete, Greece. March 2016. Available at: www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler (Retrieved July 14, 2016).

Jie Wang, A. Zachary Kissel, "Introduction to Network Security: Theory and Practice", Singapore: Wiley, 2015. ISBN 9781118939505. UIN: BLL01017585410.

Bundesamt für Sicherheit in der Informationstechnik (BSI), "The State of IT Security in Germany, 2015". Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2

F. Lantenhammer, A. Scholz, A. Seidel, A. Schuttpelz, A, "Cyber Defence und IT-Security Awareness", in, Europäische Sicherheit & Technik : ES&T. No.8,, 2012. Journal ISSN: 2193-746X. UIN: ETOCRN316565061.

T1-B2: Информационная безопасность и риски

Описание

Информационная безопасность (ИБ) в целом применяется к информации самого разного вида (частной, публичной, особо важной, с ограниченным доступом и т. д.), обращение с которой (вне зависимости от того, существует ли она в электронной или других формах) требует соблюдения определенных регламентов и правил, а также выполнения установленных требований. Слабые места в системе ИБ могут использоваться хакерами, преступниками и иностранными разведывательными службами. В данном разделе представлены общая концепция информационной безопасности и риски для нее. Основное внимание уделяется при этом компьютерным системам[4]. В течение курса обучающимся будет представлено более подробное объяснение специфики национального подхода к информационной безопасности (см. тему 4). На этом этапе мы перейдем от обсуждения критериев и способов присвоения информации статуса защищенной к проведению различия между информационной безопасностью и снижением уязвимости информации и информационных систем, после чего мы рассмотрим различные примеры слабых мест в компьютерных информационных системах и проанализируем алгоритм осуществления нападения на таковые (от обнаружения цели до ее поражения). Вслед за этим внимание будет уделено вопросам управления рисками в сфере информационной безопасности посредством таких подходов, как оценка угроз и рисков (ОУР)[5], в особенности, применительно к постоянным угрозам повышенной сложности[6]. На данном этапе учащиеся должны получить общее представление об основных национальных структурах и органах, ответственных за выработку политики, процедур и регламентов в сфере обеспечения ИБ.

Введение

ИБ включает в себя механизмы и процессы, позволяющие оценивать состояние аппаратного обеспечения и хранимых на нем или передаваемых по нему данных. Информационная безопасность занимается техническими и операционными вопросами, связанными с прикладными решениями и инфраструктурой в сфере защиты информационных систем. Снижение уязвимости информации и информационных систем (в разных странах данная концепция может иметь различные названия) включает в себя вопросы ИБ, помимо этого, в нее входят вопросы управления информацией, ее целостности и защиты, а также протоколы для сокращения рисков или общего управления ими и задачи по уменьшению последствий инцидентов. Основной целью в сфере ИБ считается, как правило, обеспечение конфиденциальности, целостности, доступности, а также подлинности и неотказуемости информации. Практические меры и режимы информационной безопасности могут осуществляться на нескольких уровнях: индивидуальном, организационном (в масштабах предприятия) и общенациональном.

Результаты обучения

В ходе освоения данного блока учащиеся получат возможность продемонстрировать свои знания и навыки в следующих областях:

- стандарты классификации безопасности в сфере информации, а также информационных и электронных систем;
- проведение на необходимом уровне анализа угроз и рисков, а также
- различные примеры алгоритмов атак в информационной среде.

Изучение учебного материала позволит:

- понять значение основных терминов, относящихся к этой теме (данные, знания, информация, информационная безопасность, алгоритм атаки в информационное среде);
- уяснить смысл снижения уязвимости информации и информационных систем, а также значение конфиденциальности, целостности, доступности, подлинности и неотказуемости информации для обеспечения безопасности информационных систем;
- объяснять роль анализа уязвимости к угрозам в рамках управления информационной безопасностью, а также
- определять организации, ответственные за формулирование государственной политики, практических мер и процедур в сфере обеспечения информационной безопасности.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки:

- Эволюция информационной безопасности
- Источники международного передового опыта
- Определение государственных органов и структур, играющих ведущую роль в обеспечении информационной безопасности в компьютерных системах

Методика обучения / Оценка результатов

Преподавание может осуществляться в формате лекций, демонстрации конкретных практических

4 Система ИБ для компьютерных систем предназначена, как минимум, для обеспечения бесперебойности работы, конфиденциальности, целостности, доступности, а также подлинности и неотказуемости информации, т. е. данная концепция направлена на гарантирование авторизованному пользователю должного доступа на необходимом уровне.

5 Как будет объяснено позже, модель ОУР предназначена для анализа информационных ресурсов, угроз, уязвимых мест и систем управления.

6 В данном контексте «повышенная сложность» означает, что угроза носит скоординированный, запланированный и изощренный характер, а понятие «постоянный» используется в значении «непрерывный». Так, постоянные угрозы повышенной сложности предполагают наличие хорошо подготовленных злоумышленников, стремящихся получить доступ к информации, изменить или исказить ее, воспрепятствовать доступу к ней, а также использовать или уничтожить компьютерные ресурсы и средства.

примеров и описания реальных ситуаций. После прохождения темы учащиеся должны знать, что такое информационная безопасность, алгоритм атаки в информационной среде, постоянные угрозы повышенной сложности, а также оценка угроз и рисков.

Учебные и справочные материалы

Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition (Indianapolis, IN: Wiley), 2008.

Управление разведки и безопасности Министерства обороны Австралии. *2015 Australian Government Information Security Manual: Controls*. Издано по указанию начальника отдела связи МО Австралии д-ра Пола Талони. 2015 г. http://www.protectivesecurity.gov.au

Управление разведки и безопасности Министерства обороны Австралии. *2015 Australian Government Information Security Manual: Principles*. Издано по указанию начальника отдела связи МО Австралии д-ра Пола Талони. 2015 г. http://www.protectivesecurity.gov.au

Объединенный центр информационной безопасности Канады. *Harmonized Threat and Risk Assessment (TRA) Methodology*, 23 октября 2007 г.

D.E. Gelbstein, *Information Security for Non-Technical Managers*, 1st Edition, 2013. ISBN 978-87-403-0488-6.

Eric M. Hutchins, Michael J. Clopperty and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington, DC, 17–18 March 2011.

Ассоциация по аудиту и контролю информационных систем (ISACA), *Advanced Persistent Threat Awareness Study Results*, USA, 2014.

Richard Kissel, ed., *Glossary of Key Information Security Terms*, NIST Interagency Report (IR) 7298 Revision 2, NIST, Computer Security Division, Information Technology Laboratory, May 2013.

Gil Klein, "Unlocking the Secrets of Cybersecurity: Industry experts discuss the challenges of hacking, tracking, and attacking in a virtual world," University of Maryland University College *Achiever* (Spring 2013): 6–20. https://www.umuc.edu/globalmedia/upload/Spring2013-Achiever.pdf

Gary Stoneburner, *NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security*, NIST, December 2001.

"Common Criteria for Information Technology Security Evaluation," accessed 17 July 2015. http://www.commoncriteriaportal.org/

Публикации Международной организации по стандартизации, посвященные информационным технологиям:

1) ISO/IEC 27001:2013 Информационные технологии – методы информационной безопасности – Системы управления информационной безопасностью - требования
2) ISO/IEC 27005:2011 Информационные технологии - методы информационной безопасности – Системы управления информационной безопасностью
3) ISO/IEC 27031:2011 Информационные технологии - методы информационной безопасности - Руководящие указания по готовности информационно-коммуникационных технологий для ведения бизнеса
4) ISO/IEC 27032:2012 Информационные технологии - методы информационной безопасности – Руководящие указания по кибербезопасности

A. Rutowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin and T. Takahashi, "CYBEX – The Cybersecurity Information Exchange Framework (X.1500)," ACM SIGCOMM Computer Communication Review, Vol. 40, no. 5, 2010. Available at: http://www.beepcore.org/p59-3v40n5i-takahashi3A.pdf

Babak Akhgar et al "Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies". Amsterdam: Butterworth-Heinemann, 2015. ISBN 9780128019733. British Library Shelfmark: General Reference Collection DRT ELD.DS.28766. UIN: BLL01017039420.

M. Watin-Augouard, "Cyber-Menaces: Un Trait Saillant du Livre Blanc", in, Administration: Revue d'étude et d'information Publiée par l'Association du Corps Préfectoral et des Hauts Fonctionnaires du Ministère de l'intérieur. No.239, 2013. Journal ISSN: 0223-5439.

H. Fukatsu, "IT Security Against Cyber Attacks; A Common Thread for Both Developed and Developing Countries", in, Nihon Igaku Ho shasen Gakkai zasshi ; Asian Oceanian Congress of Radiology; AOCR 2014; Kobe, Japan. Journal ISSN: 0048-0428. British Library Shelfmark: 6113.254000. UIN: ETOCCN087891561

Safa, Nader Sohrabi, Rossouw Von Solms, and Lynn Futcher. "Human aspects of information security in organisations." Computer Fraud & Security 2016, no. 2 (2016): 15-18.

Alshaikh, Moneer, Sean B. Maynard, Atif Ahmad, and Shanton Chang. "Information Security Policy: A Management Practice Perspective." arXiv preprint arXiv:1606.00890 (2016).

T1-B3: Структура информационного пространства: опорная сеть Интернета и сетевая инфраструктура государств

Описание

Данный учебный блок посвящен техническим аспектам информационного пространства. Основное внимание уделяется при этом глобальной инфраструктуре, а также информационным системам, созданным в масштабе государств и отдельных предприятий. Информационное пространство включает в себя архитектуру Интернета, компьютерные и мобильные сети. В этом блоке в первую очередь рассматриваются принципы общей структуры и конкретная топология Интернета в отдельных государствах (т.е. национальная инфраструктура, поддерживающая работу сетей, провайдеры телекоммуникационных услуг, а также схемы маршрутизации).

Введение

Архитектура опорной сети Интернета включает в себя ключевые каналы обмена данными между основными компьютерными сетями и магистральные маршрутизаторы. Такие сети и маршрутизаторы размещаются в коммерческих, государственных, научных и других высокомощных сетевых центрах. Эти центры управляют точками обмена Интернет-трафиком и пунктами доступа к сети и обеспечивают обмен трафиком между странами и континентами. Как правило, крупные Интернет-провайдеры (например, провайдеры первого уровня) участвуют в обмене трафиком в опорной сети Интернета на основе частных соглашений о взаимодействии телекоммуникационных сетей. Интернет-провайдеры, управляющие отдельными сегментами Интернета, называются автономными системами (AS), которые регистрируются и получают уникальный номер автономной системы (ASN). Маршрутизация между автономными системами и их достижимость обеспечиваются посредством магистральных маршрутизаторов, использующих протокол граничного шлюза (BGP). Управление отношениями между наименованиями доменов (например: www.google.com) и маршрутизируемыми адресами осуществляется с помощью системы доменных имен (DNS) и ее собственных регистрирующих органов.

Национальный Интернет-регистратор (NIR) – организация, занимающаяся под управлением международного Интернет-регистратора распределением IP-адресов (Интернет-протоколы) и других Интернет-ресурсов в масштабе страны. Правительства государств могут также регулировать деятельность Интернет-провайдеров в рамках своего экономического региона.

В настоящее время значительную часть инфраструктуры Интернета составляют мобильные сети. Такие платформы связаны с Интернетом и именуются «мобильным Интернетом». Их общая архитектура и специфика в масштабе государства являются предметом рассмотрения в этом учебном блоке.

Результаты обучения

Освоение учебного материала данного блока позволит учащимся

- развить глубокое понимание физической и виртуальной топологии опорной сети Интернета и специфики управления ею,
- объяснять значение номеров ASN для обеспечения взаимодействия различных частей Интернета во всем мире, а также объяснять функции Администрации адресного пространства Интернет (IANA),
- уяснить взаимоотношения между Интернет-провайдерами первого уровня, Интернет-провайдерами нижестоящих уровней, а также локальными сетями персональных компьютеров конечных пользователей,
- объяснять роль полномочных DNS-серверов в обеспечении взаимодействия компонентов Интернета в глобальном масштабе, а также анализировать роль Корпорации по управлению доменными именами и IP-адресами (ICANN),
- понимать топологию и географию национального киберпространства, включая роль национальных регистраторов и государственных органов, курирующих Интернет-провайдеров, и
- разбираться в структуре мобильных сетей Интернета и управлении ими, а также понимать осуществление связи между этими сетями и Интернетом в масштабах государства.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

Для эффективного начального обучения лиц, не являющихся техническими специалистами, представители учебных организаций, использующие данный справочный учебный план для подготовки конкретных курсов, должны крайне внимательно отнестись к вопросу технической сложности таких курсов, для того чтобы их материал был понятен для учащихся.

Некоторое время в ходе занятий может быть уделено информационным сетям и телекоммуникационной инфраструктуре страны.

Методика обучения / Оценка результатов

Преподавание может осуществляться в формате лекций и демонстрации конкретных практических примеров. Учебный план можно также разнообразить посещением соответствующих объектов в стране, выступлениями экспертов, а также комплексными устными и практическими экзаменационными работами.

Учебные и справочные материалы

Организация ICANN, "Beginner's Guide to Domain Names," 6 December 2010.

Администрации адресного пространства Интернет. *The IANA Functions: An Introduction to the Internet Assigned Numbers Authority (IANA) Functions*, ICANN. Июнь 2015 г.

Paul Krzyzanowski, "Understanding Autonomous Systems: Routing and Peering," 5 April 2013, accessed 17 July 2015. https://www.cs.rutgers.edu/~pxk/352/notes/autonomous_systems.html

Michael Miller, "How Mobile Networks Work," Pearson Education, Que Publishing, 14 March 2013, accessed 17 July 2015.

Ram Mohan, "Attacking the Internet's Core", SecurityWeek website, 16 March 2011, accessed 17 July 2015. http://www.securityweek.com/attacking-internets-core

Jeff Tyson, "How WAP Works," HowStuffWorks website, accessed 17 July 2015. http://computer.howstuffworks.com/wireless-internet3.htm

Rudolph van der Berg, "How the 'Net works: An introduction to peering and transit," 2 September 2008, accessed 17 July 2015. http://arstechnica.com/features/2008/09/peering-and-transit/4/

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds. The Turn to Infrastructure in Internet Governance. Springer, 2016.

Konstantinos Moulinos, Rossella Mattioli, EU ENISA, "Communication network interdependencies in smart grids", Heraklion, Crete, Greece. March 2016. Available at: www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids (Retrieved July 14, 2016).

Abdulrahman Alqahtani. "Towards a framework for the potential cyber-terrorist threat to critical national infrastructure: A quantitative study" Information and computer security. Vol 23, No 5; 2015; 532-569. Journal ISSN: 2056-4961. British Library Shelfmark: 4481.796000. UIN: ETOCvdc_100027180236.0x000001

E. Sitnikova, E. Foo, R.B. Vaughn, "The Power of Hands-On Exercises in SCADA Cyber Security Education", International Federation for Information Processing -Publications- IFIP.; Information security education; Heidelberg; Springer; 2013. Journal ISSN: 1868-4238. British Library Shelfmark: 4540.183500. UIN: ETOCCN085265877

O. Netkachov, P. Popov, K. Salako, "Quantification of the Impact of Cyber Attack in Critical Infrastructures", in, Journal on Data Semantics; Reliability and Security Aspects for Critical Infrastructure Protection, Florence, Italy, 2014; Sep, 2014, pp 316-327. Journal ISSN: 0302-9743. UIN: ETOCCN088306466.

T1-B4: Протоколы и платформы

Описание

Для обмена данными информационные системы используют четко определенные форматы сообщений, которые принято называть протоколами. Протокол передачи данных представляет собой набор правил для обмена данными в компьютере или между компьютерами (как соединенными, так и несоединенными). Протоколы можно сравнить с элементами почтового адреса на конверте с указанием отправителя, получателя и их соответствующих координат. Каждое сообщение имеет точное значение, предназначенное для получения ответа из ряда возможных ответов, заранее определенных для конкретной ситуации. Так, в протоколе должны быть установлены правила, значение и порядок обмена данными. Заданный образ действий обычно не зависит от способа передачи сообщения или различных систем, через которые оно может проходить на пути к своему адресату.

Каждый уровень протокола и процесс имеет характерные уязвимые пункты и риски, которые могут использовать злоумышленники (в зависимости от своих знаний и подготовки). При обсуждении этой темы достаточно затронуть базовые аспекты, но с учетом аудитории ее можно обсудить и применительно к уровням, представляющим собой государственную/служебную тайну.

Введение

Концепция и структура сетевой системы могут быть подготовлены двумя способами.

С логической точки зрения работа Интернета основывается на протоколах. Стеки протоколов являются формой реализации стандартов протоколов передачи данных. Стеки определяют способы упаковки и перемещения данных. Как правило, реализация протоколов осуществляется в рамках многоуровневой архитектуры (т. е. стеков). Протоколы более низких уровней выполняют простые функции передачи данных, в частности, пересылку небольшого количества данных от одного компьютера к другому в локальной сети (например, Ethernet). Протоколы более высоких уровней в стеке выполняют такие задачи, как общую адресацию в глобальных сетях (например, Интернет-протоколы), коррекцию ошибок и формирование крупных блоков данных (протоколы управления передачей (TCP)). Протоколы самых высоких уровней выполняют наиболее абстрактные задачи прикладного характера, в т. ч. доставку сообщений по электронной почте (например, простой протокол передачи почты (SMTP)) или обеспечение просмотра файлов и ресурсов на странице в Интернете (протокол передачи гипертекста (HTTP)). Более высокие уровни протоколов в стеке зависят от выполнения базовых функций на низовых уровнях.

С другой стороны, физическая архитектура Интернета описывает способы реализации протоколов сетевыми устройствами и платформами (например, коммутаторами и маршрутизаторами, шлюзами, прокси-серверами и межсетевыми экранами (файерволами)), а также формы связи таких сетевых устройств. Так, сетевые коммутаторы, обеспечивающие функционирование протокола Ethernet, могут подключать компьютеры к локальной вычислительной сети (ЛВС). ЛВС могут быть соединены с сетевыми маршрутизаторами, использующими Интернет-протоколы для переадресации пакетов данных между сетями и, возможно, с остальными сегментами Интернета. Почтовый сервер, подключенный к данной сети может использовать протокол SMTP.

Задача четкого отображения отношений между физическими устройствами и описания их роли при реализации протоколов в современных информационных системах осложняется появлением виртуальных устройств и сетей. В таких сетях устройства и их связи могут генерироваться виртуально посредством программного обеспечения, работающего на крупных серверах (как, например, в случае «облачных вычислений»). Приобретение такими системами виртуального характера добавляет еще один уровень сложности в сфере обеспечения безопасности, и это является проблемой, которая ждет своего решения.

Стеки протоколов могут создаваться для специального применения. Примерами программных пакетов, которые используются для отслеживания измеряемых параметров и отправления контрольных сообщений, являются промышленные системы управления, например, программы диспетчерского управления и сбора данных (SCADA). В системах электроснабжения они, в частности, могут отслеживать загрузку сетей и переключать подачу электричества в зависимости от изменяющегося потребления. Защищенность систем SCADA имеет большое значение для обеспечения безопасности национальной инфраструктуры, т.к. такие системы могут управлять работой объектов общегосударственного значения. Многие современные виды вооружений используют электронные системы, которые сопоставимы с промышленными платформами SCADA и поэтому тоже могут оказаться уязвимыми.

Каждый уровень протокола имеет характерные для него риски и уязвимые пункты, которыми, опираясь на свои знания и умения (как общие, так и экспертного уровня) могут воспользоваться злоумышленники.

Определение протокола сетевой безопасности

В целом протоколы сетевой безопасности обеспечивают защищенность и целостность данных во время их передачи через сетевое соединение. Протоколы сетевой безопасности определяют процессы и способы защиты данных сети. Протоколы сетевой безопасности не обеспечивают полной защиты сетей: каждый протокол предназначен для противодействия определенным образом какому-либо конкретному виду атаки на систему или сеть. Следует учитывать, что в стране или на международном уровне эти протоколы могут называться по-разному.

Часто в протоколах сетевой безопасности для защиты данных используются криптография и шифрование, благодаря которым данные могут быть расшифрованы или изменены только с помощью специального алгоритма, логического ключа, математической формулы и/или комбинации всех этих методов. Широкое распространение нашли такие протоколы сетевой безопасности, как «безопасная оболочка» (протокол SSH), протокол безопасной передачи данных (SFTP), протокол безопасной передачи гипертекста (HTTPS) и протокол уровня защищенных сокетов (SSL).

Результаты обучения

Освоение учебного материала данного блока позволит учащимся

- давать описание/участвовать в обсуждении ролей и функций каждого уровня протоколов сетевой безопасности (стеки протоколов TCP-/IP),
- давать характеристику таких общих сетевых устройств, как концентраторов (хабов), коммутаторов, маршрутизаторов, шлюзов и серверов приложений, описывать способы реализации ими уровней протоколов, а также их функцию в сети,
- обсуждать основные концепции виртуализации сетевых устройств и определяемых программным обеспечением сетей, воздействие этих концепций на архитектуру сетей и их связь со средой «облачных вычислений»,
- описывать базовые элементы управления промышленными объектами на основе SCADA (это может включать в себя конкретные компоненты управления промышленным объектами и их операционную основу в форме стандартных Интернет-протоколов), а также
- определять и описывать общие протоколы сетевой безопасности, их взаимодействие с архитектурой сетей, основанной на протоколах различных уровней, и указывать, какие конкретные уязвимые места в сети каждый из протоколов призван устранять.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

Для выявления уязвимых мест информационных систем и определения их привлекательности для нападения могут быть рассмотрены системы управления промышленными объектами (например, SCADA) и ИТ-системы военного назначения (системы PIT).

Методика обучения / Оценка результатов

Для проведения занятий по данной теме рекомендуются лекции, демонстрации примеров и изучение конкретных ситуаций. Оценка успехов должна производиться в письменной форме с учетом специфики курса, определенной на основе данного учебного плана.

Учебные и справочные материалы

Ассоциация стандартов IEEE (Институт инженеров по электротехнике и электронике), стандарты IEEE 802. http://standards.ieee.org/about/get/

Инженерный совет Интернета (IETF), запрос на комментарии (RFC). Доступ осуществлен 17 июля 2015 г. https://www.ietf.org/rfc.html

Certiology, Network Devices, accessed 17 July 2015. http://www.certiology.com/computing/computer-networking/network-devices.html

Cisco Systems Inc., Virtual LANs VLAN Trunking Protocol (VLANs VTP), accessed 17 July 2015. http://www.cisco.com/c/en/us/tech/lan-switching/virtual-lans-vlan-trunking-protocol-vlans-vtp/index.html

D. Clark, "The Design Philosophy of the DARPA Internet Protocols", *Proceedings of SIGCOMM '88*, 106–14 (New York: Association for Computing Machinery), August 1988.

Kevin R. Fall and W. Richard Stevens, *TCP/IP Illustrated, Volume 1: The Protocols*, 2nd edition, Addison-Wesley Professional Computing Series (Boston, MA: Addison Wesley Professional), 15 November 2011.

Juniper Networks, Inc., "White Paper: Architecture for Secure SCADA and Distributed Control System Networks", 2010, accessed 17 July 2015. http://www.ndm.net/ips/pdf/junipernetworks/Juniper%20Architecture%20for%20Secure%20SCADA%20and%20Distributed%20Control%20System%20Networks.pdf

Radia Perlman, "Tutorial on Bridges, Routers, Switches, Oh My!", accessed 17 July 2015. https://www.ietf.org/proceedings/62/slides/protut-0.pdf

Bart Preneel, "Internet Security Protocols," video of lecture given at SecAppDev 2013, Leuven, Belgium. https://www.youtube.com/watch?v=CZzd3i7Bs2o

Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks*, 5th edition (New York: Pearson), 27 September 2010.

E. van Baars, R. Verbrugge, R. "A communication algorithm for teamwork in multi-agent environments", Journal of Applied Non-Classical Logics, Logic and information security; Leiden, The Netherlands, 2008; Sep, 2009, 431-462, Lavoisier; 2009. British Library Shelf Mark: 4943.400000, UIN: ETOCCN074941483

C.W. Chan "Key Exchange Protocols for Multiparty Communication Services", International Symposium on Cyber Worlds; Tokyo, 2002. Conference ISBN: 0769518621. British Library Shelfmark: 4550.208900. UIN: ETOCCN046776823.

Jan Jatzkowski, Bernd Kleinjohann, "Self-Reconfiguration of Real-Time Communication in Cyber-Physical Systems", 2016. Electronic paper held at the British Library. UIN: ETOCvdc_100033448082.0x000001.

J. Ivimaa, T. Kirt, "Evolutionary Algorithms for Optimal Selection of Security Measures". Proceedings of the 10th European Conference on Information Warfare and Security at the Tallinn University of Technology Tallinn, Estonia July 7-8, 2011, pp. 172-184. Rain Ottis (eds). ISBN 9781908272065 (pbk.) UIN: BLL01015873308.

Qadir, Junaid, Arjuna Sathiaseelan, Liang Wang, and Barath Raghavan. "Approximate Networking for Global Access to the Internet for All (GAIA)." arXiv preprint arXiv:1603.07431 (2016).

T1-B5: Архитектура сетевой безопасности и управление процессом обеспечения безопасности

Описание

Настоящий тематический блок посвящен базовым аспектам архитектуры сетевой безопасности, которые включают в себя технологические и операционные решения, а также человеческие и управленческие факторы, которые оказывают влияние на форму этой архитектуры. Элементами архитектуры сетевой безопасности на национальном уровне являются механизмы и практические меры, направленные обеспечения защищенности инфраструктуры (телекоммуникационных опорных сетей), а также общенациональные фильтры контента и структуры управления кибербезопасностью. Основная цель данного блока заключается в обучении принципам проектирования/создания условий безопасности на основе такого анализа рисков, который позволит удерживать их на приемлемых уровнях. Данная сетевая архитектура должна включать в себя средства технического и физического контроля, а также соответствующие процедуры, правила и меры подготовки. В качестве примера средств технического контроля можно назвать межсетевые экраны, системы опознавания вторжений и управления журналами регистраций. Примерами средств физического контроля могут служить системы управления доступом, пожарной тревоги и регулирования влажности. Обучающиеся узнают, как осуществлять анализ рисков и разрабатывать конфигурацию систем безопасности на национальном, а также индивидуальном и организационном уровнях.

Базовые аспекты сетевой безопасности формируются с учетом общегосударственных требований и правил, различных стандартов безопасности, жизненного цикла систем, принципов проектирования, а также элементов физической архитектуры. При изучении базовых аспектов сетевой безопасности в дополнительном порядке рассматриваются концепции надлежащего управления ресурсами, объектами и физической средой, планы по управлению и гуманитарные аспекты, включая проверку сотрудников, обеспечение непрерывности функционирования, планы действий в чрезвычайных ситуациях и аспекты устойчивости информационных систем.

Введение

Создание архитектуры сетевой безопасности должно основываться на установленных правилах и требованиях. Это означает, что оно начинается с анализа находящихся в распоряжении информационных ресурсов. Центральное значение здесь отводится ценности информационных ресурсов для защищающейся стороны (т.е. степень ущерба в результате потери или изменения информации), а также ценности этих ресурсов для возможных злоумышленников. Именно такое определение информационных ресурсов и оценка их важности находятся в основе выработки требований и правил по управлению доступом к информации.

В ходе анализа угроз выявляются те субъекты, которые с большой долей вероятности могут нанести вред определенным ресурсам. Помимо этого, рассматриваются технические возможности таких злоумышленников. Создание архитектуры сетевой безопасности основывается на необходимости подготовки системы физических объектов и соответствующих критериев для снижения уязвимости информации и информационных систем, а также на разработке операционных процедур, позволяющих уменьшить риск повреждения или уничтожения имеющихся информационных ресурсов. Государства могут иметь собственные критерии и стандарты применительно к оценке угроз и рисков, а также требованиям к проектированию и порядку использования механизмов по управлению к доступу и к архитектуре сетевой безопасности.

Выбор и организация архитектуры сетевой безопасности предприятий часто основываются на принципах «эшелонированной обороны», под которой понимается координированное использование ряда решений для обеспечения целостности информационных ресурсов. Защита информационных ресурсов начинается с управления доступом к данным, на следующем уровне предусматриваются средства защиты приложений, которые осуществляют доступ к таким данным, помимо этого, предусматриваются меры защиты в хостах, на которых эти приложения установлены, а также в структуре сети предприятия и внешнем периметре безопасности предприятия (где происходит соединение корпоративной сети с глобальной сетевой инфраструктурой).

Архитектура сетевой безопасности предприятия включает в себя комплекс средств, предназначенных для снижения рисков для этого предприятия. Общими механизмами, или архитектурными элементами, сетевой безопасности являются зонирование сети, межсетевые экраны, системы обнаружения вторжений, антивирусные программы, средства шифрования и системы информации о состоянии безопасности и управления инцидентами (системы SIEM). Ни одна из этих систем не может обеспечить защищенность сетей в одиночку. Методы сетевых атак разнообразны и могут использовать уязвимые места во многих протоколах, системах и программных приложениях, что может оказать пагубное воздействие на всю инфраструктуру предприятия.

Под действиями, направленными на обеспечение защищенности сетей, понимаются меры, предпринимаемые в ходе разработки и оценки архитектуры безопасности сети предприятия. Целью при этом является гарантирование эффективности такой архитектуры. Необходимо учитывать, что в некоторых случаях меры могут оказаться скорее теоретическими, чем реальными. Так, в рекламе продукта, управляющего доступом к данными, может быть указан ряд функций обеспечения защищенности сети. Соответствующая мера безопасности может быть предусмотренной проверкой этой функции на основе признанных стандартов для подтверждения того, что продукт функционирует должным образом, без сбоев. Другими примерами мер по обеспечению сетевой безопасности могут служить официальные и полуофициальные проверки проектных решений, разработка документов по обеспечению безопасности и руководств для пользователей и операторов систем, управление жизненным циклом элементов систем безопасности и конфигурацией, управление разработчиками элементов архитектуры/управление условиями производства, а также надежная доставка элементов архитектуры от разработчика/производителя в предприятие. Помимо этого, обеспечение безопасности систем включает в себя программы по проверке благонадежности сотрудников и порядку предоставления им доступа к тайне, что необходимо для установления необходимого уровня доверия пользователей и системных операторов.

Результаты обучения

Освоение учебного материала данного блока позволит учащимся

- уяснить, каким образом комбинация уровней безопасности в эшелонированной обороне сети предприятия способна обеспечивать его защищенность в случае отказа одного из механизмов безопасности или использования злоумышленниками уязвимого места в системе;
- готовить (на базовом уровне, с подготовкой схем сетей) необходимое зонирование сети и размещение таких элементов, как межсетевых экранов;
- учитывать и понимать общенациональные стандарты и руководящие указания для проведения оценок угроз и рисков, подготовки концепций сетевой безопасности для предприятий и организаций, а также для создания архитектуры элементов безопасности сетей;
- анализировать связь этапа определения важных объектов в ходе оценки угроз и рисков (ОУР) и разработки концепции сетевой безопасности предприятия;
- уяснить соотношение этапа анализа угроз во время ОУР и выявления слабых мест в системе сетевой защиты, которые могут быть использованы злоумышленниками. Это поможет также понять, как эти факторы определяют требования к мерам безопасности, осуществляемым в сети предприятия, а также
- учитывать и понимать параметры и сферу действия общенациональной системы обеспечения секретности документов и информации, а также описывать взаимосвязь проверок благонадежности сотрудников и программ допуска к тайне.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

Для того чтобы обучающиеся могли анализировать системы сетевой безопасности, которые используются в их организациях или которые их организациям следует внедрить, представляется целесообразным обсуждение различных видов управления системной архитектурой и зонирования элементов безопасности сетей.

Предметом подробного обсуждения могут стать такие примеры мошенничества в Интернете, как манипуляция психологией человека и социальная инженерия.

Внимания может заслуживать анализ и обсуждение таких вопросов, как основная общенациональная система допуска к физическим объектам, документам и информации, а также вопросы проверки сотрудников и допуска к тайне.

Методика обучения / Оценка результатов

Преподавание может осуществляться в формате небольших рабочих групп, рассматривающих человеческие, технологические и операционные аспекты безопасности.

Выступления экспертов как из государственного, так и частного секторов могут подчеркнуть актуальность обсуждаемых тем и повысить наглядность процесса обучения.

Оценка успешности усвоения материала будет зависеть от требований, предъявляемых к конкретной группе обучающихся.

Учебные и справочные материалы

Управление разведки и безопасности Министерства обороны Австралии. *Australian Government Information Security Manual: Controls*, issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. See www.protectivesecurity.gov.au

Управление разведки и безопасности Министерства обороны Австралии. *Australian Government Information Security Manual: Principles*, issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. See www.protectivesecurity.gov.au

Deborah J. Bodeau and D.J. Graubart, "Cyber Resiliency Engineering Framework," MITRE Technical Report MTR 110237 (Bedford, MA: The MITRE Corp.), September 2011.

Объединенный центр информационной безопасности Канады. *Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)*, июнь 2007 г.

Объединенный центр информационной безопасности Канады. *Harmonized Threat and Risk Assessment (TRA) Methodology (TRA-1)*, 23 октября 2007 г.

Объединенный центр информационной безопасности Канады. *Information Technology Security Guideline: Network Security Zoning: Design Considerations for Placement of Services within Zones (ITSG-38)*, май 2009 г.

Объединенный центр информационной безопасности Канады. *Information Technology Security Guideline: User Authentication Guidance for IT Systems (ITSG-31)*, март 2009 г.

George Farah, "Information Systems Security Architecture—A Novel Approach to Layered Protection: A Case Study," GSEC Practical Version 1.4b, SANS Institute, 9 September 2004. www.sans.org

D.E. Gelbstein, *Information Security for Non-Technical Managers*, 1st Edition, 2013. ISBN 978-87-403-0488-6.

Gil Klein, "Unlocking the Secrets of Cybersecurity: Industry Experts Discuss the Challenges of Hacking, Tracking, and Attacking in a Virtual World," University of Maryland University College *Achiever* (Spring 2013): 6–20. https://www.umuc.edu/globalmedia/upload/Spring2013-Achiever.pdf

Alexander Klimburg, ed., *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn, Estonia, 2012. ISBN 978-9949-9211-2-6. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

William Pelgrin, "A Model for Positive Change: Influencing Positive Change in Cyber Security Strategy, Human Factors, and Leadership," Center for Internet Security.

Anthony Thorn, Tobias Christen, Beatrice Gruber, Roland Portman and Lukas Ruf, "What is a Security Architecture?," paper by the Working Group Security Architecture, Information Security Society Switzerland (ISSS), 29 September 2008.

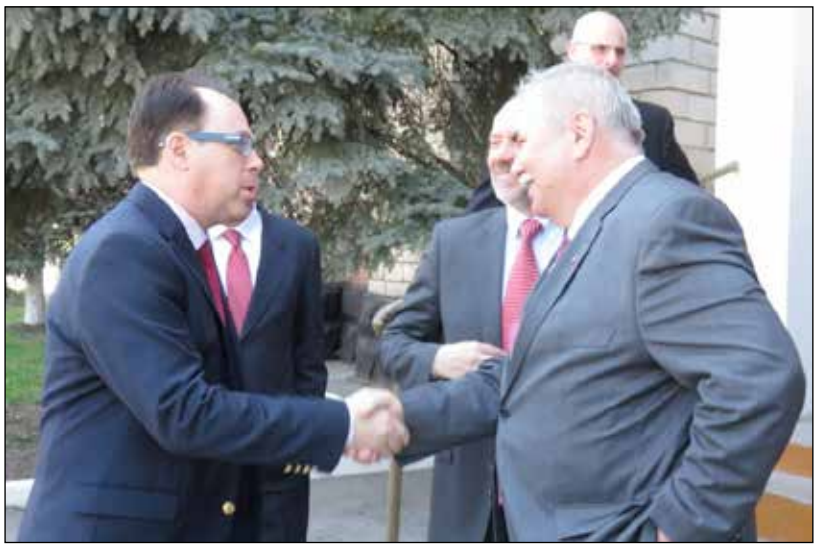
S.A. Chun, V. Atluri, B.B. Bhattacharya, "Risk-Based Access Control for Personal Data Services", Statistical Science and Interdisciplinary Research; International Conference on Information Systems Security; Algorithms, Architectures; Kolkata, India, 2006; Dec, 2009, 263-284. Journal ISSN: 1793-6195. Conference ISBN: 9789812836236; 9812836233. British Library Shelf Mark: 8448.954000. UIN: ETOCCN071364080.

Gérard Desmaretz, Cyber Espionnage, Ou, Comment Tout le Monde épie Tout le Monde!, Paris: Chiron, 2007. ISBN 9782702712122 (pbk.) UIN: BLL01014343705.

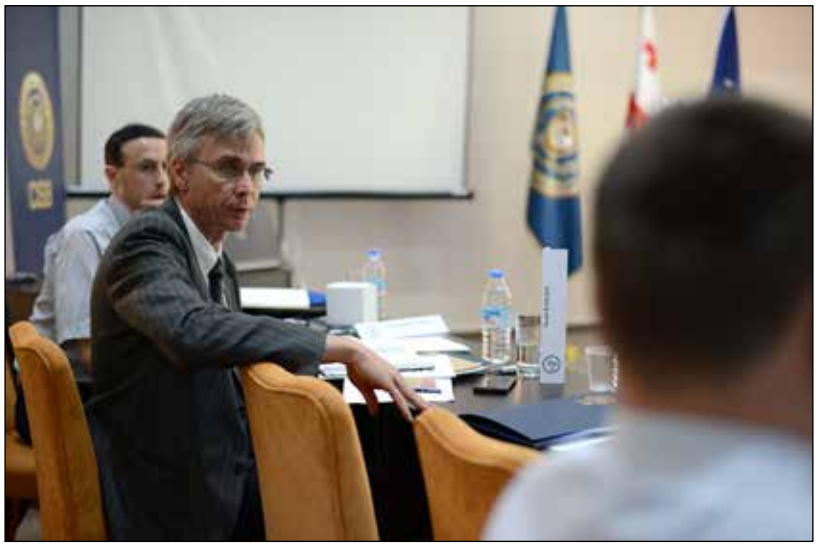
A. Rutowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin and T. Takahashi, "CYBEX – The Cybersecurity Information Exchange Framework (X.1500)," ACM SIGCOMM Computer Communication Review, Vol.40, No.5, 2010.

I. Atoum, A. Otoom, A.A. Ali, "A Holistic Cyber Security Implementation Framework" in Information Management & Computer Security, Vol.22; No 3, 2014, pp 251-264. Journal ISSN: 0968-5227. UIN: ETOCRN359424579.

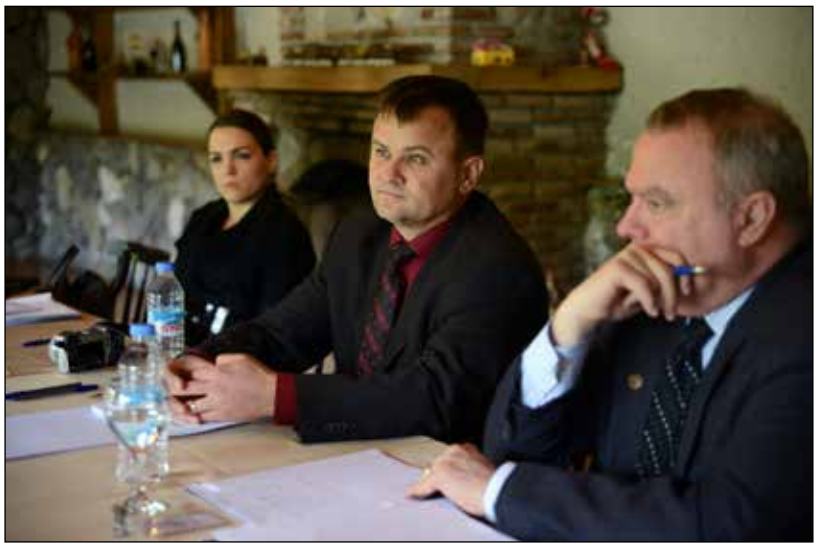
Yoo, Hyunguk, and Taeshik Shon. "Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture." Future Generation Computer Systems 61 (2016): 128-136.



В разработке Учебного руководства по кибербезопасности объединяются представители как стран-членов НАТО, так и стран, не состоящих в Альянсе. Встреча министра обороны Молдовы с редакторами.



Семинар группы составителей Учебного руководства по кибербезопасности в Тбилиси (Авторы из Гринвичского университета и Королевского военного колледжа Канады).



Семинар группы составителей Учебного руководства по кибербезопасности в Тбилиси (Авторы из Школы НАТО в Обераммергау, i-intelligence и SLCE).

Тема 2: Векторы риска

Цель

Данная тематическая область представляет вводный обзор уязвимостей, характерных для киберпространства и способов и средств для использования таких уязвимостей посредством различных схем или векторов нападения. Понимание данных уязвимостей – неотъемлемый компонент оценти риска и принципов снижения его уровня, что также будет рассматриваться.

Описание

Данный учебный план был составлен с учетом выводов, сделанных в рамках отчета Национальной группы по кибериссследованиям США, адресованного Директору Национальной разведки США, в котором утверждается, что всевозможные уязвимости в киберсфере можно разделить на категории по следующим блокам вектора риска (см. Чабински 2010 г. в Списке литературы): «цепь поставок и доступ для поставщиков»; удаленный доступ; доступ по карточкам дистанционного считывания и доступ изнутри». Таким образом, в рамках данной темы, в Разделе T2-B1 обсуждается тема Цепи поставок / Поставщиков с уделением особого внимания вопросам безопасности посредством систем контроля, начиная от производственных цехов до субподрядчиков, транспортировки, хранения и технического обслуживания; в Разделе T2-B2, Нападения с удаленного и доступа по карточкам дистанционного считывания, рассматриваются используемые уязвимости, связанные с несанкционированным (недозволенным) доступом; в Разделе T2-B3, доступ изнутри (Нападения при наличии местного доступа), рассматриваются используемые уязвимости, связанные с дозволенным доступом в систему; а также Раздел T2-B4, Риски, связанные с мобильностью, личными переносными устройствами и новыми явлениями, обсуждаются риски, связанные с правилами в отношении личных переносных устройств, интернет-технологиями типа «облако» и другими вопросами, связанными с мобильностью.

Общая цель рассмотрения данной темы заключается в предоставлении основы в вопросах уязвимостей, присущих компонентам киберпространства. Тем не менее, программа, разрабатываемая на основе данного учебного, может подразумевать обучение на экспертном уровне или в засекреченном виде с целью соблюдения текущих правил и законов на государственном уровне.

Задачи обучения

Обучаемые должны получить возможность

- понимать значительность и возможное воздействие на основе используемой цепи поставок, удаленного, внутреннего доступа и доступа по карточкам дистанционного считывания, нацеленное на уязвимости в киберпространстве и факторы, связанные с упрощением повышенной мобильности, а также
- Выявлять типы компромиссов между безопасностью и частной жизнью, связанные с повышенной мобильностью и другими векторами риска, установленными в данной тематической области.

Список рекомендуемой литературы

Steven R. Chabinsky, ”Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line,” Journal of National Security Law & Policy 4, no. 27 (August 2010): 27–39. http://jnslp.com/wp-content/uploads/2010/08/04_Chabinsky.pdf

Wenke Lee and Bo Rotoloni, Emerging Cyber Threats Report 2015, report prepared by the Georgia Tech Information Security Center (GTISC) and the Georgia Tech Research Institute (GTRI) for the Georgia Cyber Security Summit, 2014. https://www.gtisc.gatech.edu/pdf/Threats_Report_2015.pdf

Louis Marinos, ENISA Threat Landscape 2013: Overview of Current and Emerging Cyber-threats, ENISA, 11 December 2013, ISBN 978-92-79-00077-5. http://www.enisa.europa.eu, doi:10.2788/14231

Mark Mateski, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka and Jason Frye, Cyber Threat Metrics, Sandia National Laboratories, March 2012. http://fas.org/irp/eprint/metrics.pdf

Francesca Spinalieri, Joint Professional Military Education Institutions in an Age of Cyber Threat, report, Pell Center for International Relations and Public Policy, Salve Regina University, August 2013.

U.S. Office of Director of National Intelligence, Understanding Cyber Threats: A Guide to Small and Medium Sized Businesses, Intelligence Community Analyst, Private Sector Program, 2014.

ISO standards on Risk Assessment/Risk Management.

T2-B1: Система поставок/Поставщики

Описание

В данном блоке рассматривается вопрос уязвимостей в системе поставок и вводится понятие передовой практики в области управления риском в системе поставок.

Система поставок как целое известна своей уязвимостью. Мониторинг и обеспечение безопасности системы поставок может представлять значительный вызов на глобальном рынке. В контексте вызовов безопасности системы поставок рассматриваются целостность самой системы, а также качество и гарантии системы безопасности и предотвращение сбоев в работе системы, использования преступниками уязвимостей и последующие нападения. В глобальных системах поставок используются маршруты, по которым высокоточное оборудование поставляется из производственных цехов, причем, это касается как отдельных компонентов, так и готовой продукции: компьютерной техники и программного обеспечения. Системы поставок уязвимы по причине возможного прерывания цикла поставки: продукция может быть захвачена и продукция может быть подвержена изменениям, например, замене деталей на неработающие или вводе вирусов в програмное обеспечение, что может происходить на разных этапах производства, транспортировки, хранения, установки или ремонта; также в процессе утилизации может быть извлечена ценная информация. Другие элементы организационной или государственной инфраструктуры могут быть скомпрометированы в процессе поставки или по вине поставщиков, в результате чего происходит внештатные ситуации. Могут ли поставщики гарантировать безопасность на должном уровне? Что нужно сделать для обеспечения безопасности для всей системы поставок?

Перспективы обучения

Обучаемые получат возможность

- понимать основные вызовы, касающиеся полного производственного цикла;
- объяснить роль организации структуры (т.е., устройства системы) в контексте безопасности системы поставок; а также
- понимать роль и требования сформулированных правил и практики в отношении управления риском в сфере системы поставок.

Вопросы для возможных модулей обучения и подходов для рассмотрения

- Уязвимости в системе поставок перед лицом киберпреступности и шпионажа
- Подходы и передовая практика в отношении снижения риска
- Текущие правила и принципы по управлению риском в системе поставок

Методика обучения/Оценка результатов

Обучение процессу поставки может включать лекции и рассмотрение конкретных внештатных ситуаций и соответствующих последствий.

Индивидуальное задание: найдите пример внештатной ситуации в отношении системы поставок и определите способ решения проблемы.

Дополнительно: составьте схему системы поставок и определите области риска.

Список литературы

Jon Boyens, Celia Paulsen, Rama Moorthy and Nadya Bartol, Supply Chain Risk Management for Federal Information Systems and Organizations, NIST Special Publication 800-161, Second Public Draft, U.S. Department of Commerce, Washington, DC, 2014.

Steven R. Chabinsky "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Lines," *Journal of National Security Law & Policy* 4, no. 1 (2010): 27.

Trusted Computing Group. Fact Sheet. 2009. http://www.trustedcomputinggroup.org/files/resource_files/7f38fa36-1d09-3519-add14cb3d28efea6/fact%20sheet%20May202009.pdf

Luca Urciuoli, Toni Männistö, Juha Hinsta and Tamanna Kahn. "Supply Chain Cyber Security—Potential Threats," *Information & Security: An International Journal* 29, no. 1 (2013): 51–68. http://www.ndm.net/ips/pdf/junipernetworks/Juniper%20Architecture%20for%20Secure%20SCADA%20and%20Distributed%20Control%20System%20Networks.pdf

U.S. Government Accountability Office, "Addressing Potential Security Risks of Foreign-Manufactured Equipment," testimony of Mark L. Goldstein, Director, Physical Infrastructure Issues, before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives, U.S. Government Accountability Office, GAO-13-652T, 21 May 2013. http://www.gao.gov/assets/660/654763.pdf

ISO 28000 Standards statements.

Emmanouil Tranos, Peter Nijkamp, Karima Kourtit “The Death of Distance Revisited: Cyber-Place, Physical and Relational Proximities”, Journal of Regional Science, Vol.53, No.5, 2013. Journal ISSN: 1467-9787.

E. Anyefru, “Cyber-Nationalism: The imagined Anglophone Cameroon Community in Cyberspace”, in African Identities, Vol.6, No.3, (2008), pp 253-274. Journal ISSN: 1472-5843. British Library Shelfmark: 0732.501500. UIN: ETOCRN234554771

A. Almalawi, X Yu, Z Tari, A. Fahad, I. Khalil, “An Unsupervised Anomaly-Based Detection Approach for Integrity Attacks on SCADA systems”, in Computers & Security. Vol. 46, (2014), pp 94-110. Journal ISSN: 0167-4048 . British Library Shelfmark: 3394.781000. UIN: ETOCRN359669860 .

Y Li, L Shi, P Cheng, J Chen, D.E. Quevedo, “Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach”, IEEE Transactions on Automatic Control. Vol.60; No.10, 2015. Journal ISSN: 0018-9286. UIN: ETOCRN375325720.

A. Sokolov, V. Mesropyan, A. Chulok, A, Aje, “Supply Chain Cyber Security: A Russian outlook”, Technovation: an International Journal of Technical Innovation and Entrepreneurship. 2014. Vol 34; No. 7; 2014, 389-391. Journal ISSN: 0166-4972. British Library Shelfmark: 8761.150000. UIN: ETOCRN353289650.

Florin Gheorghe Filip, Luminita Duta, “Decision Support Systems in Reverse Supply Chain Management”, Elsevier Paper, 2015. UIN: ETOCvdc_100030799942.0x000001.

Dmitry Ivanov, Alexandre Dolgui, Boris Sokolov, Boris, Frank Werner, Marina Ivanova, “A Dynamic Model and an Algorithm for Short-Term Supply Chain Scheduling in the Smart Factory Industry 4.0”, in International Journal of Production Research, Vol.54, Issue 2, (2016); 2016; pp 386-402. Journal ISSN: 0020-7543. (Electronic). Britsh Library Shelfmark: ELD Digital store 4542.486000. UIN: ETOCvdc_100031962439.0x000001

J. Sztipanovits, et al. “OpenMETA: A Model-and Component-Based Design Tool Chain for Cyber-Physical Systems”, in Journal on Data Semantics. No. 8415, (2014), pp 235-248. Journal ISSN: 0302-9743. UIN: ETOCRN350535700.

Lu, Tianbo, Xiaobo Guo, Bing Xu, Lingling Zhao, Yong Peng, and Hongyu Yang. “Next Big Thing in Big Data: The security of the ict supply chain.” In Social Computing (SocialCom), 2013 International Conference on, pp. 1066-1073. IEEE, 2013.

T2-B2: Нападения из удаленного доступа и доступа по карточкам дистанционного считывания

Описание

Кибернападения могут быть либо удаленными, либо локальными. Последние можно разделить на те, что совершаются посредством получения доступа по карточкам дистанционного считывания к системам или же могут совершаться лицом, имеющим санкционированный доступ. Нападения такого вида рассматриваются отдельно в Разделе T2-B3. Понятие удаленного доступа охватывает все методы и подходы, используемые для нарушения работы сетей, где отсутствует очевидный физический доступ к компьютерному обеспечению системы. При удаленном нападении, злоумышленник мог не иметь прежнего физического доступа к системе, которая подвергается нападению; злоумышленник получает доступ через сеть или иное устройство связи, причем нападающий может не иметь ранее полученного санкционированного доступа к системе. Напротив, в контексте локальных нападений, злоумышленник как правило имеет доступ к системе или в ней в определенной форме, пытаясь повысить свой уровень привилегированного доступа для получения несанкционированной формы или степени доступа к информации. Подобная деятельность, осуществляемая злоумышленником, не имеющим санкционированного доступа, будет рассматриваться в данном документе в контексте нападения с помощью доступа по карточкам дистанционного считывания. По объяснению Чабински (2010 г.), «нападение с доступа по карточкам дистанционного считывания» касается возможности злоумышленника нарушить деятельность, осуществить перехват или другим способом внедриться в сеть и компьютерные системы, находясь в непосредственной близости к различным элементам, таким как стационарные компьютеры, кабели или беспроводные принимающие устройства. Доступ по карточкам дистанционного считывания является формой удаленного доступа. Распространенные методы, такие как беспроводное «зондирование» (перехват и доступ к информации, отправляемой по беспроводным сетям), фиксирование информации по нажатию на клавиши клавиатуры, снимок содержимого экрана, перехват информации с помощью посредника и внедрение вредоносной программы физическими средствами – все это способы применения злоумышленниками доступа по карточкам дистанционного считывания с использованием уязвимостей.

В данном разделе рассматриваются нападения как с удаленным доступом, так и доступом по карточкам дистанционного считывания (которые не являются нападениями лицами с санкционированным доступом). Данный раздел призван отметить самые распространенные риски, связанные с нападениями как с удаленным доступом, так и доступом по карточкам дистанционного считывания и обсудить различные средства по избежанию или противостоянию таким действиям.

Введение

В контексте классических сетевых программ, существует понятие клиента и сервера. «Клиентская» компьютерная программа отправляет запросы на «серверскую» программу в соответствии с определенным протоколом, запрашивая информация или выполнение действия. Взаимодействие всегда начинает клиент. Сервер ожидает связи по некоторому известному адресу сети. Протоколы, контролирующие данное поведение, включают сетевые службы (HTTP или HTTPS), службы по передаче файлов (FTP) и службы системы электронной почты (SMTP, POP3 или IMAP). Удаленные нападения могут быть нацелены на уязвимости сервера (ошибки программного обеспечения или конфигурации), которые позволяют нападающему получить доступ к информации из компьютера сервера или даже контролировать его на удалении.

Удаленные нападения со стороны сервера могут осуществляться, если злоумышленнику удастся выявить ошибку в конфигурации или програмном обеспечении на самом сервере. К примеру, ошибка в конфигурационных настройках может позволить нападающему ввести заведомо ошибочный режим обслуживания системы, что дает возможность широкого доступа к системе. Другим примером является нападение на веб-сервер HTTP, в котором есть внутренняя база данных для предоставления ресурсов данных. Заведомо ошибочные запросы злоумышленником на веб-странице могут предоставить ему возможность отправки опасных для системы последовательностей команд на внутреннюю базу данных, что дает возможность злоумышленнику получить над ней контроль. Такой тип нападения называется «Внедрение SQL (Языка структурированных запросов).”

В свете сложности обеспечения более совершенной защиты для серверов (брандмауэры, контроль доступа и т.п.), акцент сместился от нападения на сервер к нападению на клиентские приложения. Тем не менее, прямой контакт с клиентскими приложениями в сети исключен, поскольку именно с помощью самих приложений всегда инициируется обмен информацией. Таким образом, злоумышленник должен найти способ обманом заставить пользователя клиентским приложением связаться с вредоносным сервером, который может причинить ущерб клиентскому приложению во время взаимодействия. Подобная деятельность по

заманиванию пользователей в ловушку, имеющая множество названий, является явным способом обмана на основе получения доверия оператора и его определенных действий, например, открытие приложения к электронному посланию, содержащее вредоносную программу.

Перспективы обучения

Основная цель данного раздела – убедиться в том, чтобы слушатели получили представление обо всем спектре рисков, связанных с нападениями из удаленного доступа, а также доступа по карточкам дистанционного считывания.

Обучаемые смогут:

- понимать и иметь возможность описать сценарий нападения на основе удаленного доступа, выявить составные части такого нападения и сопоставить это со сценариями нападения на основе доступа по карточкам дистанционного считывания;
- ознакомиться со структурой приложений на основе взаимодействия клиента с сервером, а также их сетевой топологией, а также иметь возможность определить, насколько для этой модели подходят обычные протоколы, такие как HTTP, HTTPS, FTP и протоколы электронной почты;
- уметь объяснить как в рамках нападения со стороны сервера получается информация на этапе сбора данных с применением методов, таких как анализ уязвимостей сети и анализа граничных значений, а также объяснить, почему инструменты для анализа уязвимости сети имеют ценность как для нападающего, так и для защитника;
- иметь основное представление о сценариях нападения со стороны сервера, например, использование слабых конфигураций, имитация ИП (IP), обеспечение отказа / дистрибутивного отказа в обслуживании (DoS и DDoS), внедрение SQL и переполнение сетевого буфера на основе протоколов;
- описать как укрепление безопасности на сетевом периметре и усовершенствование безопасности на сервере привели к разработке и распространению методов нападения со стороны клиента;
- иметь основное представление о сценариях нападения со стороны клиента, таких как межсайтовый скриптинг (внедрение выполняемых на клиентском компьютере вредоносных скриптов в выдаваемую системой страницу), подделка межсайтовых запросов, использование веб-браузеров в своих целях и документы, содержащие вирус Троян; и
- уметь определить и обсудить отношения между нападениями со стороны клиента и методами действий на основе обмана, такими как нападения типа «фишинг» (phishing) и нападения на предприятие или отрасль, когда заражается сайт, часто посещаемый сотрудниками данного предприятия.

Вопросы для возможных модулей обучения и подходов для рассмотрения

- Степень технической сложности рассматриваемых вопросов может сильно варьироваться на основе наличия времени и технической осведомленности обучаемых.
- Исследование различных видов нападения с применением методов обмана пользователей

Методика обучения/Оценка результатов

Процесс обучения может включать лекции и демонстрацию на основе примеров. В докладах текущих сетевых администраторов можно рассказать о постоянных устойчивых угрозах. Реальные примеры из практики страны должны выявляться и формулироваться для иллюстрации практических и непосредственных проблемы. Необходимо разработать разнообразные практические меры оценки в зависимости от уровня подготовки обучаемых и поставленных учебных задач.

Список литературы

Steven R. Chabinsky, “Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Lines,” *Journal of National Security Law & Policy* 4, no.1 (2010): 27.

Shirley Radack, ed., *Information Technology Laboratory Bulletin: Log Management: Using Computer and Network Records to Improve Information Security*, 1, 2 (October 2006), National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. http://csrc.nist.gov/publications/nistbul/b-10-06.pdf

Murugiah Souppaya and Karen Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NIST Special Publication 800-83, Revision1, U.S. Department of Commerce, July 2013. http://dx.doi.org/10.6028/NIST.SP.800-83r1

U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team, *Using Wireless Technology Securely*, US-CERT, 2008. http://www.us-cert.gov/reading_room/Wireless-Security.pdf

Emmanouil Tranos, Peter Nijkamp, Karima Kourtit "The Death of Distance Revisited: Cyber-Place, Physical and Relational Proximities", Journal of Regional Science, Vol.53, No.5, 2013. Journal ISSN: 1467-9787.

E. Anyefru, "Cyber-Nationalism: The imagined Anglophone Cameroon Community in Cyberspace", in African Identities, Vol.6, No.3, (2008), pp 253-274. Journal ISSN: 1472-5843. British Library Shelfmark: 0732.501500. UIN: ETOCRN234554771

A. Almalawi, X Yu, Z Tari, A. Fahad, I. Khalil, "An Unsupervised Anomaly-Based Detection Approach for Integrity Attacks on SCADA systems", in Computers & Security. Vol. 46, (2014), pp 94-110. Journal ISSN: 0167-4048 . British Library Shelfmark: 3394.781000. UIN: ETOCRN359669860 .

Y Li, L Shi, P Cheng, J Chen, D.E. Quevedo, "Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach", IEEE Transactions on Automatic Control. Vol.60; No.10, 2015. Journal ISSN: 0018-9286. UIN: ETOCRN375325720.

T2-B3: Вторжение в систему лицами, обладающими доступом (Нападения при наличии локального доступа)

Описание

Нападение с помощью компьютьера на информационную систему или сеть осуществляется с использованием уязвимости в системе или компьютерной программе для выполнения вредоносного действия с целью нанесения ущерба конфиденциальности, целостности или наличию информации. Такие «вторжения» можно поделить на удаленные и локальные. В случае с локальным вторжением, нападающими уже был установлен доступ к системе, которая подвергается нападению—то есть, они уже имеют привилегированный доступ к системе и нападения являются попытками повысить уровень привилегированности для получения несанкционированного доступа к информации. В данном разделе рассматриваются нападения на основе локального доступа. Злоумышленники, имеющие физический доступ к системе или возможность воспользоваться ими, могут нанести значительный ущерб операции, компании или организации. Они могут делать это за деньги, из мести или ввиду претензий или идеологических соображений. Однако есть вероятность, что ущерб или утеря информации может произойти в результате ошибки оператора или по причине халатности.

Введение

«Привилегия» в сфере компьютерной безопасности – это разрешение на выполнение действия. В данном случае, разрешение является правом конкретного пользователя на доступ к конкретному ресурсу системы, например, файлу или программе, на применение определенных команд системы или для получения доступа к конкретной услуге, например, сетевому устройству. Как правило, контроль над уровнем привилегий пользователя регулируется посредством установки личности пользователя в электронном виде и применении набора правил контроля доступа (протоколов) которые управляют выполнением действий по прочтению, написанию и программированию пользователем в системе. Злоумышленник может попытаться «повысить уровень привилегированности» и получить доступ к большему объему информации путем получения контроля над «идентификационными данными» другого пользователя (часто путем захвата программы, управляемой пользователем с высоким уровнем привилегий) или путем модификации внедренных протоколов безопасности. Если злоумышленники получают достаточный уровень привилегий, они могут получить административный контроль над системой. Нападающий в этом случае может быть авторизованным пользователем системы—злоумышленник, действующий «изнутри», пытающийся выполнить недозволенные действия. В другом случае, нападающий может оказаться сторонним лицом, осуществляющим удаленное нападение для получения идентификационных данных пользователя с ограниченными привилегиями. Получив точку доступа, нападающий может с помощью похищенных данных пользователя осуществить локальное вторжение для повышения своего уровня привилегий, получая более широкий доступ. В принципе, есть сложность отличить один сценарий от другого, поскольку в обоих из них фигурируют нападения с локальным доступом и многие методы снижения угрозы схожи.

Один из основных принципов ограничения уровня уязвимости от нападений с локальным доступом это предоставление информации исключительно на основе служебной необходимости. Принцип «наименьшей привилегированности» применим к разработке и выполнению правил и политики в отношении контроля доступа, чтобы пользователь получал доступ только к ресурсам, необходимым в рамках служебных обязанностей. Данное понятие также включает принцип «разделения обязанностей» — например, один и тот же администратор не может внести изменения в политику безопасности и также утвердить их.

Разделение полномочий также часто применяется для ограничения воздействия в результате нападений на основе местного доступа. Зонирование сетевой безопасности является эффективным методом разделения полномочий. Сетевое зонирование применяется для снижения риска путем разделения служб инфраструктуры на логические элементы, имеющие схожие правила безопасности при передаче информации и такие же требования к безопасности. Зоны разделяются на периметры безопасности, вводимые посредством сетевый устройств безопасности (брандмауэры, IDS, программы по предотвращению утери данных).

Учитывая спектр уязвимостей, рассматриваемых в этом разделе, необходимо осмыслить логику программ и процедур, направленных на снижение уровня уязвимостей, характерных для доступа в систему на основе предотвращения, обнаружения или сдерживания. Подобные меры будут рассмотрены более подробно в других разделах данного учебного плана.

Перспективы обучения

Обучаемые смогут

- демонстрировать знание о существовании угроз организации, которые могут исходить от ее сотрудников;

- описать нападения на основе локального доступа и выявять составные части такого нападения;
- объяснить разницу между нападением на основе удаленного и локального доступов;
- продемонстрировать понимание различия между понятиями «разрешение» и «привилегия» и как они используются для контроля доступа пользователей к информационным ресурсам системы;
- проявить базовые знания методов, применяемых нападающими для злоупотребления своими текущими привилегиями и повышения их уровня;
- объяснить применение принципов наименьшего уровня привилегий и служебных обязанностей, а также разработки политики безопасности на их основе; а также
- указать, как структурировать информацию на основе здравой политики зонирования сетевой безопасности.

Вопросы для возможных модулей обучения и подходов для рассмотрения

- Политика и программы для подготовки персонала, проверки на благонадежность, уменьшение угрозы и общая осведомленность о проблемах, присущих физическому доступу к системам и ее элементам – все эти вопросы необходимо усвоить в рамках данного раздела, однако степень детальности рассмотрения данных вопросов может варьироваться.
- Заинтересовать обучаемых можно на основе проработки реальных ситуаций.
- Можно обсудить инструменты для выявления наличия угрозы в сети и определения ее качеств.

Методика обучения/Оценка результатов

Рекомендуются лекции на основе конкретных примеров и их наглядное иллюстрирование.

Необходимо обсудить конкретные случаи, сценарии на основе примеров и рассмотреть такие случаи с точки зрения судебной экспертизы.

Предложение для более комплексного упражнения: обучаемые, работая в группах, должны найти и проанализировать реальные примеры нападения злоумышленником, имеющим санкционированный доступ и предложить способы избежания проблемы. Обучаемые могут взять за основу пример действий злоумышленника, имеющего санкционированный доступ и злоупотребляющего своими полномочиями для нанесения ущерба тем ресурсам, к которым у него нет доступа по принципу служебной необходимости.

Методы оценки должны зависеть от уровня знаний обучаемых, который они должны продемонстрировать в соответствии с целями обучения и выполнения работы, установленные для конкретной программы, в рамках которой они обучаются.

Список литературы

Centre for the Protection of National Infrastructure, "Insider misuse of IT systems," May 2013. https://www.cpni.gov.uk/documents/publications/2013/2013008-insider-misuse_of_it_systems.pdf?epslanguage=en-gb; also see "Cyber Insiders," https://www.cpni.gov.uk/advice/cyber/Cyber-research-programmes/Cyber-insiders/

Communications Security Establishment Canada, *Information Technology Security Guideline: Network Security Zoning: Design Considerations for Placement of Services within Zones* (ITSG-38), May 2009. https://cse-cst.gc.ca/en/system/files/pdf_documents/itsg38-eng_0.pdf

P.A. Legg et al., "Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection," Cyber Security Centre, Department of Computer Science, University of Oxford, 2013. https://www.cpni.gov.uk/documents/publications/2014/2014-04-16-insider_threat_detection.pdf?epslanguage=en-gb

Jason R.C. Nurse et al., "Understanding the insider threat: A framework for characterising attacks," *IEEE 2014 Security and Privacy Workshops*. https://www.cpni.gov.uk/documents/publications/2014/2014-04-16-understanding_insider_threat_framework.pdf?epslanguage=en-gb or http://www.ieee-secrity.org/TC/SPW2014/papers/5103a214.pdf

S. Sagan and M. Bunn, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge MA: American Academy of Sciences), 2014, ISBN 0-87724-097-3. https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderthreats.pdf

Derek A. Smith, National Cybersecurity Institute, "The Insider Threat," video. https://www.youtube.com/watch?v=z-CDyZdcGck

U.S. Department of National Defense, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security and Special Activities*, DoDM 5105.21-V3, 19 October 2012. http://www.dtic.mil/whs/directives/corres/pdf/510521m_vol3.pdf

Verizon Enterprise Solutions, "2015 Data Breach Investigations Report." www.verizonenterterprise.com

Markus Kont, Mauno Pihelgas, Jesse Wojtkowiak, Lorena Trinberg, Anna-Maria Osula, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015 ""Insider Threat Detection Study"". Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Insider_Threat_Study_CCDCOE.pdf

P. Gola and G. Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 5th ed., Cologne, 2009

F. Schwand, "Wenn Mitarbeiter Unternehmens-Laptops privat nutzen, besteht Regelungsbedarf," acant.service GmbH, 23 April 2014. [Online]. Available: http://www.acantmakler.de/2014/04/23/unternehmen-laptops-private-nutzung/. [Accessed 14 September 2015]

Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon), "Isikuandmete töötleminetöösuhetes," 2011. [Online]. Available: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhe

Deutscher Bundestag, "Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes," 15 December 2010. [Online]. Available at: http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf

T2-B4: Риск, связанный с мобильностью, личные мобильные устройства и новые тенденции

Описание

Переход общества на мобильные средства связи необратим, в то время как последствия этого феномена для безопасности недостаточно изучены. Более того, рост популярности социальных сетей (например, Фейсбук и Твиттер) меняет схему межличностного и глобального общения. Информация об активности частных и юридических лиц, распределенное управление доступом с персональных устройств без должной защиты в системы безопасности, коммерческих перевозчиков и подобные, а также новые элементы представляют риск для целостности засекреченных данных и систем. К примеру, потеря или кража компьютера типа «ноутбук» или мобильного телефона с электронными данными, документами или ссылками могут быть опасными для частных и юридических лиц, а также для государства. В данном разделе рассматриваются вопросы безопасности, связанные с данными тенденциями.

«Пользуйтесь личным мобильным устройством» - политика компании, разрешающая сотрудникам пользоваться личными мобильными устройствами («ноутбуками», «планшетами» и мобильными телефонами) на своем рабочем месте и пользоваться этими устройствами при выполнении служебных обязанностей для получения доступа к закрытой информации и программам. Данная политика порождает конфликт интересов между организацией, чья политика безопасности призвана обеспечивать конфиденциальность и целостность информационных ресурсов, а также защиту сотрудников, которые желают сохранять владение устройством и личными данными и избежать мониторинга. Организации должны устанавливать правила и применять практику для ситуаций, когда сотрудник увольнятся или в случае потери, кражи или продажи устройства во избежание использования незащищенного устройства злоумышленниками для получения сетевого доступа к системе предприятия. Использование системы «облако» для хранения информации представляет аналогичную проблему с контролем доступа и конфигурации.

Введение

Общая практика предприятий в отношении безопасности сводится к построению тщательно зонированной архитектуры безопасности и создания контролируемых «точек отсечения» для управления доступом в интернет. Политика использования собственных устройств со входом в интернет приводит к появлению новых точек доступа, которые скорее всего, не будут контролироваться в рамках политики безопасности предприятий. Это базовый принцип компьютерной безопасности, когда целостность нижних уровней обычно рассматривается как аксиоматичная в отношении верхних уровней. Это исключает изменение пользователями реализации принципов политики безопасности в отношении корпоративных программ на личных мобильных устройствах. Другими словами, корпоративные системы безопасности (программы и т.п.) не могут быть установлены на личное устройство на постоянной основе по причине обладания пользователем административного контроля над устройством, которое (к примеру, личный смартфон), нельзя обезопасить только лишь путем установления программ или инструментов обеспечения безопасности. Есть ряд методов, которые позволяют обеспечить безопасности личных мобильных устройств или ограничивают риск, который они представляют. В основе таких методов лежит структура безопасности, которая ограничивает доступ с устройства к сети предприятия, а также информацию, которую можно перенести на такое устройство. Принципы зонирования, которые обеспечивают сегментацию и сегрегацию сети могут обеспечить мобильность в работе и относительно безопасную стратегию использования личных устройств в рабочих целях. Тем не менее, решения, подразумевающие более высокую степень безопасности, ставят под вопрос возможность распространенного применения личных устройств.

Помимо этого, переход к применению инфраструктуры, предоставляемой в качестве услуги через технологию «облака» приводит к потенциальной утрате базовой архитектуры безопасности и принципов обеспечения безопасности. Мобильные устройства сами создают потоки данных, которые могут представлять интерес для иностранных разведслужб и коммерческих предприятий. Пользование соцсетями также приводит к возможному использованию личной информации пользователей, которая была выложена в соцсети самими пользователями или открыта для доступа / хранится на их мобильных устройствах, раскрывая массу информации (личный статус, мнения, местонахождение, привычки) которой могут воспользоваться злоумышленники. Подобные соцсети могут также представлять потенциальную угрозу, служа проводником в различные ИТ-системы, делая их уязвимыми для вирусов или вторжений. Соцсети также могут служить эффективным средством для распространения пропаганды и дезинформации, привлечения широкой общественности, отправки множественных сообщений для мобилизации народных масс и подобной деятельности.

Перспективы обучения

Обучаемые смогут

- Продемонстрировать понимание положительных и отрицательных аспектов в отношении компромисса между политикой безопасности и пользованием соцсетями на работе с точки зрения работника и работодателя;
- анализировать политику мобильности и использования личных устройств на работе в контексте архитектуры безопасности предприятия, а также определить компромисс между безопасностью и пользовательскими правами; и
- анализировать политику в отношении использования «облаков» при хранении и обработке информации (например, медицинские карты, правительственные/военные данные) в государственном и международном контекстах.

Вопросы для возможных модулей обучения и подходов для рассмотрения

- Возможности злоумышленников будет обсуждаться в подробностях с целевой аудиторией.
- Привлечение внимания к необходимости вносить изменения в среду безопасности в соответствии с развитием технологий.
- Конкретные требования и ограничения для мобильных платформ связи, включая применение собственных устройств.
- Конкретные требования и ограничения по использованию «облака».
- Внедрение передовой практики в структуру предприятия на основе международной и государственной практики.
- Использование злоумышленниками личной информации о пользователе, размещаемой в соцсетях — Обсуждения на тему пользованием поисковой системой Гугл (Google) с последующим практикумом.

Методика обучения/Оценка результатов

Обучение может включать презентации, дискуссии в общем составе, работу в группах и обсуждение конкретных случаев.

Требуется проводить постоянную оценку качества и активности обсуждения вопросов в общем составе и группах.

Список литературы

W. Arbaugh, D. Farber and J. Smith, "A Secure and Reliable Bootstrap Architecture," *Proceedings of the 1997 IEEE Symposium on Security and Privacy* (Oakland, CA) 1997, 65–71.

D.P. Cornish, "Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks," EU DG-For External Policies of the [European] Union Directorate B—Policy, February 2009. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

Ravi Gupta and Hugh Brooks, *Using Social Media for Global Security* (Indianapolis, IN: John Wiley & Sons), 2013, ISBN 978-1-118-44231-9.

Zeb Hallock et al., *Cisco Unified Access (UA) and Bring Your Own Device (BYOD) CVD*, Cisco Systems, Inc., revised 28 August 2014, accessed 30 July 2015. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.pdf

Raytheon Corp., *Security in the New Mobile Ecosystem*, Ponemon Institute Research Report, August 2014.

Murugiah Souppaya and Karen Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST Special Publication 800-124, Revision 1, NIST, U.S. Department of Commerce, June 2013. http://dx.doi.org/10.6028/NIST.SP.800-124r1

U.S. DNI Defense Cyber Crime Center, *Countering Identity Theft Through Education and Technology*, October 2014.

U.S. Federal CIO Council and U.S. Department of Homeland Security, National Protection and Program Directorate, *Mobile Security Reference Architecture*, 23 May 2013. https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf

N. Mastali and J. I. Agbinya, "Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: A survey paper," in 2010 Fifth International Conference on Broadband and Biomedical Communications (IB2Com), 2010.

H. Kärkkäinen, "Apple myy Suomessa vaarallisia puhelimia - ja sulkee kauppiaiden suut," 30 October 2014. [Online]. Available: http://www.digitoday.fi/tietoturva/2014/10/30/apple-myy-suomessa-vaarallisia-puhelimia--ja-sulkee-kauppiaiden-suut/201415103/66. [Accessed July 2016]"

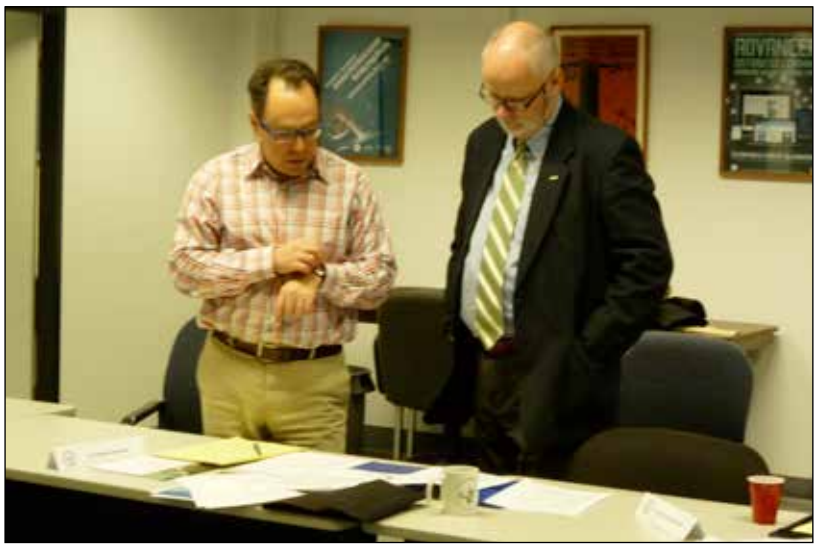
Teemu Väisänen, Alexandria Farar, Nikolaos Pissanidis, Christian Braccini, Bernhards Blumbergs, and Enrique Diez. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015 "Defending mobile devices for high level officials and decision-makers". Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Defending%20mobile%20devices%20for%20high%20level%20officials%20and%20decision-makers.pdf

Gabriele Costa, Merlo Alessio, Luca Verderame, Konrad Wrona, "Developing a NATO BYOD Security Policy", 2016 International Conference on Military Communications and Information Systems (ICMCIS). IEEEm Brussels, Belguim, May 23-24, 2016. DOI: 10.1109/ICMCIS.2016.7496587. Available at: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=7496587&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7496587

Ree C. Ho , Hiang K. Chua, "The Influence of Mobile Learning on Learner's Absorptive Capacity: A Case of Bring-Your-Own-Device (BYOD) Learning Environment", in, Taylor's 7th Teaching and Learning Conference 2014 Proceedings, Singapore: Springer,2015. pp471-479. 2015. DOI: 10.1007/978-981-287-399-6_43. Print ISBN: 978-981-287-398-9. Online ISBN: 978-981-287-399-6.

Suri, Niranjan, Mauro Tortonesi, James Michaelis, Peter Budulas, Giacomo Benincasa, Stephen Russell, Cesare Stefanelli, and Robert Winkler. "Analyzing the applicability of Internet of Things to the battlefield environment." In 2016 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1-8. IEEE, 2016.

Porche III, Isaac R. Emerging Cyber Threats and Implications. RAND Corporation, 2016.



Редакторы Учебного руководства по кибербезопасности.

Семинар группы составителей Учебного руководства по кибербезопасности в Гармише (Авторы из Чешской Республики, Соединенного Королевства и США).

Семинар группы составителей Учебного руководства по кибербезопасности в Тбилиси.

Тема 3: Международные организации по кибербезопасности, принципы и стандарты

Цель

Широкая целеустановка данной темы заключается в знакомстве участников курса с международными стандартами и такими организациями, как Национальный институт стандартов и технологий США и Британский институт стандартов (и, может, другими организациями), а также образами взаимодействия их в рамках национального контекста. Слушатели будут в состоянии определить роль организаций по международным стандартам, а также познакомятся с крупными международными организациями, роль и функции которых связаны с кибербезопасностью. Кроме того, они должны будут проанализировать свою национальную политику в области кибербезопасности в свете международных стандартов и рекомендуемого опыта, сравнивая их с различными примерами национальных принципов. Наконец, в этом тематическом блоке будут затронуты развивающиеся международные правовые режимы кибербезопасности.

Описание

Каждая страна должна адаптировать этот блок к своим потребностям, определив свои национальные организации, отвечающие за политику и практику кибербезопасности, а также поняв, как они воздействуют на соответствующие принципы кибербезопасности и структуры. Несмотря на различие в деталях, характерных для каждой страны, подход для презентации данной темы может быть выбран следующий: Т3-В1, международные организации по кибербезопасности, играющие важную роль в национальном контексте; Т3-В2, международные стандарты и требования — обзор структур и применяемых практик; Т3-В3, национальные концепции кибербезопасности с акцентом на сравнительный анализ национальных концепций и концепций других стран; и Т3-В4, кибербезопасность в национальном и международном праве.

Перспективы обучения

Речь идёт о развивающейся теме в области политики безопасности, различного рода национальные и международные ответы на вызовы кибербезопасности формируются в существующих, а также в новых организациях. Будучи комплексной национальной проблемой, кибербезопасность нуждается в политике и координации на высоком уровне, но национальные подходы являются довольно разнообразными.

Изучая развивающуюся практику государств, разрабатывающих национальную политику в отношении кибербезопасности на правительственном, коммерческом и индивидуальном уровне, а также оказывающих поддержку негосударственным актёрам в развитии способов урегулирования рисков и угроз, учащиеся должны

- Осознать, что национальные и международные ответы требуют того или иного подхода с международным участием;
- Определить главные национальные организации, отвечающие за кибербезопасность;
- Определить и понять роль и требования национальных и международных ведомств по стандартам;
- Понять важность отношений между кибербезопасностью, спецслужбами и военными институтами;
- Быть в состоянии проанализировать национальные подходы и национальную политику в свете международных стандартов и накопленного положительного опыта;
- Понять роль ключевых международных организаций, играющих лидирующую роль в кибербезопасности; и
- Познакомиться с развивающимися международными правовыми рамками и официальной политической позицией национального правительства в рамках данного развивающегося режима.

Предлагаемые источники

European Union External Action, “EU International Cyberspace Policy”. http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm

IT Governance Ltd., “Information Security & ISO 27001: An Introduction,” IT Governance Green Paper, October 2013.

Klimburg, Alexander, ed., *National Cyber Security Framework Manual*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2012.

National Institute of Standards and Technology, U.S. Department of Commerce, *Security and Privacy Controls for Federal Information Systems and Organizations*, Joint Task Force Transformation Initiative, NIST Special Publication 800-53, Revision 4, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

PricewaterhouseCoopers LLP, “Why you should adopt the NIST Cybersecurity Framework,” May 2014. https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

The White House, *Cyberspace Policy Review*. https://www.whitehouse.gov/cyberreview/documents

U.S. Government Accountability Office, *Report to Congress: Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606, July 2010.

Т3-В1: Международные организации по кибербезопасности

Описание

Количество международных организаций, правительственных и неправительственных, занимающихся проблемами глобальной или региональной кибербезопасности, велико и продолжает расти. Сферы их интересов распространяются от инвестигативного до нормативного, законодательного и политического содействия, надзора, а также включают в себя ряд других вопросов. Работа многих из этих организаций направлена на коллективные подходы по решению проблем кибербезопасности, в то время как другие более детально посвящают себя национальным или коммерческим целям. По различным причинам, их разнообразные рекомендации должны рассматриваться критически.

Вебсайт Центра киберзащиты НАТО в Таллине (CCD COE), https://ccdcoe.org/, является хорошим источником ссылок на многие региональные ведомства, связанные с политикой и практикой кибербезопасности в широком смысле слова. Сюда относятся Европейский Союз (см., в частности, о работе Европейского агентства по сетевой и информационной безопасности ENISA (https://www.enisa.europa.eu/)), Организация по безопасности и сотрудничеству в Европе, ОБСЕ (http://www.osce.org/), Организация Объединённых Наций (http://www.un.org/en/index.html) и, конечно, НАТО (http://www.nato.int/). Кроме этих источников существуют также такие организации, как Глобальный форум групп реагирования на инциденты и обеспечения безопасности (www.first.org), Международное многостороннее партнёрство против киберугроз (IMPACT), а также Ассоциация специалистов по связи и радиоэлектронике вооружённых сил (AFCEA). ENISA ведёт и регулярно актуализирует список организаций стран-членов ЕС по реагированию на киберкризисы, а также компьютерных групп реагирования на чрезвычайные ситуации (CERTs).

Прочие международные структуры, связанные с кибербезопасностью, включают в себя Международную организацию по стандартизации (см. блок 2 этой темы), Корпорацию по управлению доменными именами и IP-адресами (ICANN), Форум по управлению интернетом (IGF), а также работающий под эгидой ООН Международный союз электросвязи (МСЭ).

В настоящем блоке речь прежде всего пойдёт о том, как правительства взаимодействуют с этими многочисленными международными организациями и внедряют методы работы, базирующиеся на рекомендациях этих организаций.

Перспективы обучения

Будучи специалистами, связанными с кибербезопасностью, учащиеся должны быть в состоянии

- Сформулировать различные проблемы, касающиеся правительств и их взаимодействия с международными организациями;
- Обозначить крупнейшие международные организации, их руководящие принципы и их роль в информировании, а также поддержке национальной кибербезопасности;
- Обозначить национальные организации, отвечающие за международное сотрудничество и содействие.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

Для определения наиболее важных для той или иной страны международных структур, к которым страна может обращаться за советом и через которые она может выразить свою обеспокоенность, необходимо привлечение национального профильного специалиста.

Другие темы для обсуждения могут быть такими:

- Ключевые международные структуры, играющие важную роль для распространение информации о национальном опыте: ЕС, НАТО, правительство США (киберкомандование и т.д.) и Европол (см. www.europol.europa.eu/ec3)
- Как национальные интересы пересекаются с международными организациями и их целями
- Определение положительных и отрицательных аспектов в подходах международных организаций к кибербезопасности
- Национальные мероприятия и механизмы для решения международных проблем
- Интернет, использующийся в целях транснациональной преступности / терроризма / организованной преступности

Методика обучения / Оценка результатов

Методика обучения может включать в себя анализ актуальных проблем. Учащиеся должны исследовать и анализировать практические примеры реакции международных организаций, а также изучать тенденции международных проблем и воздействия их на развитие стран.

Оценка будет производиться в рамках группового проекта, включающего в себя аудиторские занятия и письменное задание по теме реакции международных организаций на вызовы кибербезопасности.

Ссылки

Takeshi Takahashi, Youki Kadobayashi, “Reference Ontology for Cybersecurity Operational Information”, Computer Journal Vol.50, No 10, 2014. Journal ISSN: 1460-2067.

Farzan Kolini, Lech Janczewski, “Cyber Defense Capability Model: A Foundation Taxonomy”, (2015). CONF-IRM 2015. Proceedings. Paper 32. Available at: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2015

Feng Xie, Yong Peng, Wei Zhao, Yang Gao, Xuefeng Han, “Evaluating Industrial Control Devices Security: Standards, Technologies and Challenges”, in, Computer Information Systems and Industrial Management, pp624-635, 2014. Springer Berlin Heidelberg. DOI: 10.1007/978-3-662-45237-0_57.Print ISBN: 978-3-662-45236-3. Online ISBN:978-3-662-45237-0.

Akinola Ajijola, Pavol Zavarsky, Ron Ruhl, “A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012”. Paper presented at the ‘World Congress on Internet Security (WorldCon)’ 2014. pp66-73. 10.1109/WorldCIS.2014.7028169. Available from the IEEE at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7028169&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7028169

В дополнение к упомянутым выше сетевым ресурсам, см. следующее:

N. Choucri, S. Madnick and J. Ferwerda, “Institutions for Cyber Security: International Responses and Global Imperatives,” *Information Technology for Development* 20, no. 2 (2013): 96–121. http://dx.doi.org/10.1080/02681102.2013.836699

Т3-В2 Международные стандарты и требования — обзор структур и практических действий

Описание

В данном тематическом блоке учащимся предлагается ряд международных стандартов, используемых организациями по развитию стандартов. Учащиеся должны понять роль международных технических стандартов и требований. Они познакомятся с набором стандартов ИСО (Международной организации по стандартизации), а также COBIT (Задачи управления для информационных и смежных технологий), ISACA (Ассоциация по аудиту и контролю информационных систем) и ITIL (международная библиотека инфраструктуры информационных технологий). В дискуссиях будет обсуждаться работа Национального института стандартов и технологий США (NIST), Британского института стандартов (BSI), Федерального управления по информационной безопасности ФРГ и Международной организации специалистов по безопасности ASIS (а также другие стандарты по возможности и пожеланиям). Целью обсуждения является выявление типов стандартов, а также проблем, связанных с их реализацией и с наличием конкурирующих стандартов. Кроме того, данный тематический блок обращается к теме национального подхода в отношении соблюдения международных стандартов. Наконец, он исследует границы стандартов и выявляет причины, по которым военные, оборонные или иные государственные организации могут назначать свои собственные стандарты.

Перспективы обучения

Учащиеся будут

- Понимать роль международных технических стандартов и требований;
- В состоянии определить международные организации по развитию стандартов (напр., ISO, NIST);
- В состоянии обозначить источники международных стандартов с целью их учёта в национальной киберстратегии;
- Понимать вызовы и сложности, связанные с реализацией международных стандартов
- Знать, как и какой структурой разработаны, поддерживаются и распространяются стандарты кибербезопасности, существующие в организации учащихся.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

Могут включать в себя следующее:

- Национальные и принятые национальным государством международные стандарты, непосредственно относящиеся к кибербезопасности
- Связанные с ними национальные процедурные или организационные стандарты
- Вызовы и сложности, возникающие в ходе реализации международных стандартов

Методика обучения / Оценка результатов

Способы и методы оценки должны соответствовать уровню подготовки, установленному для конкретных курсов и уроков, исходя из данной справочной программы.

Национальный эксперт подведёт итог различных стандартов, взятых на вооружение данной страной, и объяснит их отношение к существующим международным или только появляющимся стандартам в области кибербезопасности.

Учащиеся найдут и проанализируют практические примеры реализации международных стандартов.

Планируется групповая дискуссия о проблемах реализации международных стандартов. Примеры могут быть взяты, исходя из опыта работы на местах.

Ссылки

Iñigo Barreira, Izenpe, Jerome Bordier, SEALWeb, Olivier Delos, Arno Fiedler, Nimbus Technologieberatung GmbH, Tomasz Mielnicki, Gemalto, Artur Mięki na, Polish Security Printing Works, Jon Shamah, EJ Consultants, Clemens Wanko, TUV Informationstechnik GmbH, Clara Galan Manso, ENISA, Sławomir Górniak, ENISA, “Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards”, EU ENISA, July 1, 2016. Available at: https://www.enisa.europa.eu/publications/tsp_standards_2015

Manmohan Chaturvedi , Abhishek Narain Singh , Manmohan Prasad Gupta, Jaijit Bhattacharya , (2014) “Analyses of issues of information security in Indian context”, Transforming Government: People, Process and Policy, Vol. 8 Issue: 3, pp.374 - 397. DOI (available at):

http://www.emeraldinsight.com/doi/abs/10.1108/TG-07-2013-0019

L. Zhang, Q. Wang, B.Tian, "Security Threats and Measures for the Cyber-Physical Systems", in, The Journal of China Universities of Posts and Telecommunications, Vol. 20, Supp.1, 2013, pp25-29. Journal ISSN: 1005-8885. UIN: ETOCRN339930374

Blaž Markelj, Sabina Zgaga, "Comprehension of Cyber Threats and their Consequences in Slovenia", in, Computer Law & Security Review: The International Journal of Technology Law and Practice. Vol. 32. Issue 3 (2016). Journal ISSN: 2212-473X (Electronic - British Library ELD Digital store). UIN: ETOCvdc_100032209717.0x000001.

Shackelford, Scott, Scott L. Russell, and Jeffrey Haut. "Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks." UC Davis Business Law Journal (2016).

ISACA, *European Cybersecurity Implementation: Overview*, ISACA Whitepaper, 2014. http://www.isaca.org or http://www.isaca.org/knowledge-center

ISACA, European Cybersecurity Implementation Series: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/european-cybersecurity-implementation-series.aspx; see also ISACA's reports on Resilience, Risk Guidance, Assurance and Audit programs.

PricewaterhouseCoopers LLP, *Why you should adopt the NIST Cybersecurity Framework*, May 2014. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

Steve Purser, "Standards for Cyber Security" in M.E. Hathaway (ed.), *Best Practices in Computer Network Defense: Incident Detection and Response* (Amsterdam: IOS Press), 2014, 97–106. doi:10.3233/978-1-61499-372-8-97

Прочие серии стандартов (в дополнение к ISO 27000):

- ISO 9000 (менеджмент качества)
- ISO 22300 (управление непрерывностью бизнеса)
- ISO 31000 (менеджмент риска)
- BSI PAS 555

Т3-В3: Национальные рамки кибербезопасности

Описание

Будучи национальной проблемой, выходящей за рамки традиционных границ между правительством, промышленностью и гражданами, кибербезопасность нуждается в высоком уровне стратегии и координации. Принимая во внимание взаимозависимость систем, многие правительства осознали, что им необходим всеправительственный подход для управления безопасностью их собственных оперативных систем, не говоря уже о помощи в уменьшении рисков для промышленности и граждан. Однако национальные меры очень разнообразны. Некоторые страны создали национальные структуры, отвечающие за управление национальной кибербезопасностью, в то время как другие страны сделали координационные структуры, отвечающие за формулировку национальной политики, оставив при этом вопросы менеджмента и реализации стратегии в ведении различных государственных управлений. При этом другие страны интенсивно пытаются найти надлежащие рамки.

Многие правительства пошли дальше, не только формулируя или поддерживая меры кибербезопасности с целью защиты государственного аппарата, но и включили эту тему в список национальных рисков, предпринимая таким образом попытки поддержать или внедрить передовой опыт на благо частного сектора и граждан. Поддержка или санкционирование подобных мер, в частности, имеют место, когда речь идёт о защите критической инфраструктуры, которая зачастую находится в частном владении. Несмотря на это есть некоторые общие требования, как, например, определение структурных ролей и подотчётности путём издания официальных технических правил, распределения ролей и обязанностей с целью минимизации риска и адекватного реагирования на актуальные проблемы.

Данный тематический блок направлен на то, чтобы учащиеся понимали политику, стратегии и структуры кибербезопасности их страны. Учащиеся должны быть проинформированы о рамках политической стратегии их государства (если таковая имеется) и об организациях, отвечающих за национальные инструкции и технические спецификации. Учащиеся будут сравнивать различные национальные и международные документы и подходы в области стратегии кибербезопасности с целью лучшего их понимания и анализа сфер риска и ответственности.

Перспективы обучения

Учащиеся должны быть в состоянии

- Обозначить организации, отвечающие за их национальную политику кибербезопасности;
- Определить ключевые элементы национальной политики безопасности;
- Определить ответственные организации и понять их роль в разработке и выпуске технических правил / директив;
- Определить ключевые элементы технических правил / директив;
- Обсудить источники передового опыта в организации национальной кибербезопасности и
- Критически проанализировать их национальный подход, сравнив его с базисными рамочными концепциями.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

- Подход к кибербезопасности – централизованный или многосторонний
- Национальные подходы к сотрудничеству, координации и взаимодействию
- Международные организации: роли и взаимодействие в национальном контексте
- Базисные рамочные концепции — рассмотрение различных примеров

Методика обучения / Оценка результатов

Способы и методы оценки должны соответствовать уровню подготовки, установленному для конкретных курсов и уроков, исходя из данной справочной программы.

Методика преподавания может включать в себя дискуссию, лекции профильных специалистов, сравнительный анализ практических примеров, определение передового опыта, а также посещение местных структур кибербезопасности.

Ссылки

Defense Science Board, U.S. Department of Defense, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, January 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

George Farah, *Information Systems Security Architecture: A Novel Approach to Layered Protection—A Case Study*, GSEC Practical Version 1.4b, SANS Institute, 9 September 2004. www.sans.org

Alexander Klimburg, ed., *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn, Estonia, 2012, ISBN 978-9949-9211-2-6. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, report by NIST Joint Task Force Transformation Initiative, NIST Special Publication 800-53, Revision 4, NIST, U.S. Department of Commerce, Washington, DC, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

Organisation for Economic Co-operation and Development (OECD), *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, 2012. http://oe.cd/security

Sławomir Górniak, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, Jon Shamah, Sławomir Górniak, "Governance Framework of the European Standardization: Aligning Policy, Industry and Research, v1.0", Heraklion, Greece, ENISA, 2015, ISBN 9789292041540.

Tomas Minarik, "National Cyber Security Organisation: Czech Republic", 2nd Revised Ed, Tallinn, 2016. NATO CCD COE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZE_032016.pdf

Vytautas Butrimas, "National Cyber Security Organisation: Lithuania", Tallinn, 2015. NATO CCD COE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf

Lea Hriciková, Kadri Kaska, "National Cyber Security Organisation: Slovakia", Tallinn, 2015. NATO CCD COE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SLOVAKIA_042015.pdf

Lehto, Martti, and Jarno Limnéll. "Cyber Security Capability and the Case of Finland." In European Conference on Cyber Warfare and Security, p. 182. Academic Conferences International Limited, 2016.

Т3-В4: Кибербезопасность в национальном и международном законодательстве

Описание

Юридический ландшафт кибербезопасности – понятие комплексное и быстро изменяющееся. Существуют споры касательно применимости уже существующих и только развивающихся международных и национальных законов, относящихся к проблемам и вызовам кибербезопасности. Также существует широкая палитра подходов, как государства рассматривают кибербезопасность в рамках внутреннего законодательства. Некоторые государства имеют специфические законы по кибербезопасности, у других они отсутствуют. Вызов идентификации — сложности, связанные с установлением источника враждебной, угрожающей или нелегальной кибер-активности – объединяет проблемы, существующие и во внутренней, и во внешней сферах.

Формируется подборка литературы по международному и национальному праву, касающемуся кибербезопасности. Данный блок даёт учащимся обзор международных и национальных законов, отвечающих за спектр проблем кибербезопасности. Многие страны и организации в их рамках являются субъектом законов о комплаенсе, т.е. законов, требующих сообщать об определённых типах финансовых трансакций или утечке данных. Существуют также формирующиеся международные юридические и правоохранительные нормы и практики (такие, как режимы сотрудничества, учреждённые Интерполом). Юридические обязательства сообщать о киберинцидентах были приняты многими странами, кроме того предпринимаются попытки создания международного кода киберэтики. Международная координационная структура или организация, следящая за юридическими аспектами кибербезопасности, однако, отсутствует.

Учащиеся ознакомятся с национальными позициями касательно внутреннего и международного законодательства, имеющего значение для киберпространства. Акцент при этом будет сделан на кибер-безопасности. Важными внутренними аспектами являются при этом личная сфера, обеспечение функционирования системы, соблюдение нормативных требований, а также возможные последствия для коммерческого страхования в рамках появляющихся национальных и международных правовых режимов.

Перспективы обучения

Учащиеся будут

- Определять ключевые вызовы и источники стратегий в международном киберзаконодательстве;
- В состоянии объяснить юридическую ответственность участвующих сторон и нормативных актов и
- Знать национальные правовые нормативные акты, касающиеся кибербезопасности (если таковые имеются) и определять ключевые правовые органы в рамках соответствующих организаций.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

- Такие темы, как спорный правовой статус кибератак, осуществляемых государственными и негосударственными актёрами, киберпроблемы во внутреннем законодательстве, требования комплаенса со стороны организаций и индивидуальные правовые обязанности, могут быть рассмотрены в определённом объёме.
- Изучение дебатов о международном кодексе поведения в области информационной безопасности, представленном ООН.
- Внутренние правила комплаенса
- Коммерческое страхование и ответственность за киберриски.

Методика обучения / Оценка результатов

Лекции должны быть разработаны при сотрудничестве с ответственными юридическими представителями, которые могут определённо представлять свою национальную позицию по данным вопросам.

Должны быть изучены практические примеры международных и национальных юридических ответов на инциденты в области кибербезопасности.

Краткий письменный анализ, относящийся к изученным детальным материалам, должен быть составлен в качестве инструмента оценки.

Ссылки

Dan Arnaudo, "Research Note: The Fight to Define U.S. Cybersecurity and Information Sharing Policy," ASA Institute for Risk & Innovation, 2013. http://www.anniesearle.com/research.aspx?topic=researchnotes

Nils Melzer, *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research (UNIDIR), Geneva, 2011. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

NATO, *Legal Gazette: Legal Issues Related to Cyber* 35 (December 2014). This issue addresses, in separate articles, (1) legal aspects of cybersecurity and cyber-related issues affecting NATO; (2) active cyber defense to responsive cyber defense; and (3) an exploration of the threshold of "armed attack" and related legal issues of attribution and participation in cyber warfare. https://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

NATO Cooperative Cyber Defence Centre of Excellence (Michael N. Schmitt, General Editor), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press), 2013. https://ccdcoe.org/tallinn-manual.html

Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?," *Stanford Law & Policy Journal* 25 (2014): 269–299.

Hong XU. "Cyber law in China" Alphen aan den Rijn: Kluwer Law International, 2010. ISBN 9789041133335. British Library Shelfmark: YC.2011.a.9251. UIN: BLL01015641102

Radziwill Yaroslav, "Cyber-Attacks and the Exploitable Imperfection of International Law." Leiden: Brill Nijhoff, 2015. ISBN 9789004298330.

Anna-Maria Osula and Henry Rõigas (eds), International Cyber Norms: Legal, Policy & Industry Perspectives (2015). NATO CCD COE. E-Book. Full Book Available at: https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html

Zeinab Krake, Sheikha Lubna Al Qasimi, Cyber Security in Developing and Emerging Economies, 2010, Cheltenham: Edward Elgar Publishing.

Fidler, David P., Richard Pregent, and Alex Vandurme. "NATO, Cyber Defense, and International Law." Journal of International and Comparative Law 4, no. 1 (2016): 1.

Saran, Samir. "Striving for an International Consensus on Cyber Security: Lessons from the 20th Century." Global Policy 7, no. 1 (2016): 93-95.

Тема 4: Менеджмент кибербезопасности в национальном контексте

Цель

Широкой целью данной темы является изучение практики менеджмента кибербезопасности в национальном контексте.

Описание

Подходы по урегулированию проблем национальной кибербезопасности существенным образом отличаются в зависимости от страны. Хотя вызовы и методы реагирования на них могут отличаться в своих деталях, общие проблемы будут схожи во всех странах. Национальные рамки кибербезопасности могут иметь специфические различия, но в общем и целом комплексный режим зачастую включает в себя следующие проблемы, нуждающиеся в активном урегулировании и координации: (1) информационно-технологическое управление ресурсами; (2) менеджмент контроля; (3) конфигурация систем и конфигурация и конфигурация управления изменениями; (4) идентификация и менеджмент уязвимостей; (5) управление инцидентами; (6) менеджмент непрерывности услуг; (7) идентификация угроз и менеджмент решения проблем; (8) внешние зависимости и менеджмент взаимосвязей; (9) подготовка и информированность и (10) поддержание владения ситуацией[7].

Настоящая тема глубоко раскрывает методы работы в области менеджмента кибербезопасности и представляет уровень национальной готовности в области безопасности с контекстом рамок риска. В частности, в разделе T4-B1, национальные методы работы, принципы действия и организации по киберустойчивости, подробно анализируются вопросы планирования в случае возникновения чрезвычайных обстоятельств и в процессе восстановления после произошедших киберинцидентов, чтобы свести к минимуму связанную с этим дестабилизацию ситуации. В разделе T4-B2, Национальные структуры кибербезопасности, представлены национальные методы менеджмента кибербезопасности, включающие операции, реагирование на чрезвычайные ситуации и минимизацию риска. Раздел T4-B3, киберфорензика, покажет учащимся инструменты, методы и процедуры в области форензики с целью сбора, анализа и интерпретации данных с целью установления атрибуции и для спецслужб. Раздел T4-B4, Контроль и оценка безопасности на национальном уровне, представит учащимся передовой опыт оценки готовности в области национальной кибербезопасности.

Перспективы обучения

Учащиеся будут

- Понимать системный подход в процессе планирования с целью устойчивости в отношении угроз, атак и аналогичных происшествий;
- В состоянии создавать практические условия для задействования устойчивых систем в рамках национального контекста;
- В состоянии проанализировать универсальность рамок и матриц для планирования и делегирования полномочий и
- Знать распространённые типы национальных организаций реагирования и ознакомятся с ролью, требованиями и структурой их сегодняшних национальных систем, а также организаций по урегулированию организационных инцидентов и кризисов.

Предлагаемые ссылки

Deborah J. Bodeau and Richard Graubart, *Cyber Resiliency Engineering Framework*, MITRE Technical Report MTR 110237, The MITRE Corporation, September 2011. https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

Mohamed Dafir Ech-Cherif El Kettani and Taïeb Debbagh, "A National RACI Chart for an Interoperable 'National Cyber Security' Framework," *Proceedings of the European Conference on Information Warfare & Security*, January 2009.

Nicole Falessi, Razvan Gavrila, Maj. Ritter Kleinstrup and Konstantinos Moulinos, *National Cyber Security Strategies: Practical Guide on Development and Execution*, European Network and Information Security Agency, December 2012. https://www.enisa.europa.eu

Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem*, Full Report, ENISA, April 2011.

Anthony Thorn, Tobias Christen, Beatrice Gruber, Roland Portman and Lukas Ruf, "What is a Security Architecture?," paper by the Working Group Security Architecture, Information Security Society Switzerland, 29 September 2008.

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide*, Carnegie Mellon University, February 2014.

See resources at Carnegie Mellon University CERT Software Engineering Institute, CERT-RMM (CERT Resilience Management Model): www.cert.org/resilience/rmm.html

7 Derived from the Carnegie Mellon CERT-RMM.

T4-B1: Национальные методы работы, принципы действия и организации по киберустойчивости

Описание

Кибербезопасность выходит за пределы многих организационных границ. Целый ряд стран взяли на вооружение комплексный, всеправительственный подход, определяющий роли и ответственность за менеджмент киберустойчивости. Киберустойчивость направлена на обеспечение оперативности национальной киберинфраструктуры в экстренном режиме работы, а также на быстрое и эффективное её восстановление после перебоя. Ставя целью обеспечение устойчивости, данный раздел обращается к практике работы стран и организаций в сравнительном контексте.

В данном разделе учащиеся обратятся к ряду примеров комплексного подхода к проблеме кибербезопасности в таком виде, как она формулируется в опубликованных инструкциях высокого уровня (напр., в Великобритании или Соединённых Штатах) с целью анализа сильных и слабых сторон их национальной политики. Национальные направления политики, играющие роль для группы присутствующих учащихся, будут сравниваться и противопоставляться друг другу. В частности, дискуссия должна повернуться в направлении анализа существующих политических методов и практик, направленных на предотвращение, защиту, реагирование и устранение последствий киберинцидентов. Также должны быть обсуждены такие меры, как проверка, контроль и средства независимого анализа.

Перспективы обучения

Студенты будут

- В состоянии интерпретировать национальные документы по киберустойчивости;
- В состоянии сделать вклад в развитие и расширение национальных мер по обеспечению киберустойчивости;
- В состоянии определить роли и сферы ответственности индивидуумов и организаций, отвечающих за национальную киберустойчивость;
- Понимать проблемы, связанные с координацией кибероперациий во время кризисных ситуаций и
- Понимать процесс анализа решений, используемый в ходе принятия решений в рамках комплаенса во случае возникновения кризисных ситуаций.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

Национальный профильный специалист должен проанализировать существующие национальные методы действий с целью установления надлежащего уровня информации для использования во время планирования занятий.

Методика обучения / Оценка результатов

Методы обучения могут включать в себя лекции, демонстрацию наглядных примеров, посещение сайтов, а также письменные упражнения. Оценка должна включать в себя как письменные, так и устные контрольные задания.

Ссылки

Национальный профильный специалист должен будет собрать воедино надлежащие национальные инструкции и ссылки. Кроме того, существуют следующие ссылки более общего содержания:

Deborah J. Bodeau and D.J. Graubart, *Cyber Resiliency Engineering Framework*, MITRE Technical Report MTR 110237 (Bedford, MA: The MITRE Corp.), September 2011.

Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem*, Full Report, ENISA, April 2011.

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide*, Carnegie Mellon University, February 2014.

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Question Set with Guidance*, Carnegie Mellon University, February 2014.

See resources at Carnegie Mellon University's CERT Software Engineering Institute CERT-RMM (CERT Resilience Management Model): www.cert.org/resilience/rmm.html

Clausewitz Gesellschaft; Bundesakademie für Sicherheitspolitik. "Sicherheitspolitik im Cyber-Zeitalter: Reicht passive Abwehr aus?" Bonn, Germany: Mittler Report Verlag, 2014, British Library Identifier: 016828758. Document Supply Number: 3829.361655 UIN: BLL01016828758

Guido Nannariello, “E-commerce e tutela del consumatore: indagine sui codici di condotta ed i processi di certificazione”, Ispra: Joint Research Centre, Institute for the Protection and Security of Citizen, Cybersecurity Sector, 2001. UIN: BLL01011092147.

F. Cassim, “Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players”, in, Comparative and International Law Journal of Southern Africa, Vol.44, No.1, 2011, pp123-138 (University of South Africa). Journal ISSN: 0010-4051. UIN: ETOCRN296687880.

N. Shirazi, “A Framework for Resilience Management in the Cloud”, in, Elektrotechnik und Informationstechnik, Vol. 132; No.2, 2015, pp122-132. Journal ISSN: 0932-383X. UIN: ETOCRN370071353.

Kallberg, Jan. “Assessing India’s Cyber Resilience: Institutional Stability Matters.” Strategic Analysis 40, no. 1 (2016): 1-5.

T4-B2: Национальные структуры кибербезопасности

Описание

В данном тематическом блоке учащимся объясняется стратегия кибербезопасности и её реализация в контексте менеджмента кибероперациий, урегулирования киберинцидентов национального уровня, а также менеджмента факторов риска национальной кибербезопасности. Акцент должен быть сделать на концепции, помогающей распределять ресурсы, определять организационные роли и обязанности, а также уточнять действия по линии иерархической цепочки, связанные с ответственностью и отчётностью.

Опираясь на международные и национальные стандарты, в данном тематическом блоке рассматриваются основы и концепции безопасности, обращаясь при этом к комплексным основам определения ролей и обязанностей с целью урегулирования рисков кибербезопасности и реагирования на инциденты кибербезопасности. Такого рода основы зачастую отражаются в матрицах полномочий по методу ИОКИ (исполнитель, ответственный, консультант, информируемый). Инструменты матрицы полномочий находят также применение в процессе менеджмента операций кибербезопасности. Пример графика ИОКИ будет использован в качестве учебного примера. Учащиеся ознакомятся с общими принципами использования таких инструментов, прежде чем обратиться к матрицам их национальной ответственности и реагирования. Если возможно, будут также рассмотрены и проанализированы актуальные инструменты национальной политики по регулированию такого распределения полномочий и задач. В ходе дискуссии речь пойдёт об инструментах поддержки принятия решений, менеджмента риска, а также принципах, практических подходах и зонах ответственности. Несомненно, учащиеся проанализируют концепцию делегированного управления в области кибербезопасности, принятую их национальным правительством или, по крайней мере, их организацией.

Устойчивость киберсистемы может включать в себя следующее: учёт основных средств, управление контролем за управлением проекта, конфигурацию и регулирование изменений, менеджмент угроз и уязвимых сторон, планирование и менеджмент непрерывности обслуживания, менеджмент факторов внешней зависимости, обучение, а также ознакомление лиц и организаций с активным урегулированием владения ситуацией.

Перспективы обучения

Учащиеся будут

- Понимать концепцию планирования и распределения полномочий в рамках матрицы ответственности;
- Анализировать широкий спектр тем, связанных с реализацией их национальной стратегии кибербезопасности;
- Понимать, как осуществляется процесс координации действий с национальным командованием по реагированию на инциденты и контрольными структурами;
- Понимать суть менеджмента распределения полномочий в рамках кибероперациий на национальном уровне;
- Понимать, как происходит урегулирование киберрисков в контексте национальной политики и
- Понимать положительные и отрицательные аспекты концепций формального менеджмента ресурсов в отношении национального контекста кибербезопасности.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

Обсуждаемые темы могут касаться системы ИОКИ или аналогичных инструментов матрицы ответственности за урегулирование инцидентов и менеджмента восстановления и реагирования.

Методика обучения / Оценка результатов

Профильный специалист должен разработать краткий обзор методов (напр., графики ИОКИ), прежде чем определить, где существуют национальные или организационные полномочия, а также отчётливое руководство к действию. Эксперт может затем идентифицировать те из них, которые имеют непосредственное отношение к особенностям работы учащегося.

Схема оценки должна соответствовать уровню подготовки, установленному для конкретных курсов и уроков, исходя из данной справочной программы.

Ссылки

Paul Cichonski, Tom Millar, Tim Grance and Karen Scarfone, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, Special Publication NIST 800-61, Revision 2, U.S. Department of Commerce, August 2012.

Mohamed Dafir Ech-Cherif El Kettani and Taïeb Debbagh, "A National RACI Chart for an Interoperable 'National Cyber Security' Framework," *Proceedings of the European Conference on Information Warfare & Security*, 2009.

Responsibility Charting (RACI). http://www.thecqi.org/Documents/community/South%20Western/Wessex%20Branch/CQI%20Wessex%20-%20RACI%20approach%207Sep10.pdf

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Question Set with Guidance*, Carnegie Mellon University, February 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

Международные организации по стандартам ISO 22300 series и ISO 27000 series—см. список ранее.

IU. V. Nesteriak, "Державна информаційна політика Україны: теоретико-методологічны засади", Kiev, Ukraine, 2014. Monograph. ISBN 9789666193554. UIN: BLL01017709318.

Francis Domingo, "Cyber Policy in China", Europe-Asia Studies, 2015. DOI: 10.1080/09668136.2015.1102519. Available at: http://www.tandfonline.com/doi/full/10.1080/09668136.2015.1102519

Tuija Kuusisto, Rauno Kuusisto, "Leadership for Cyber Security in Public-Private Relations", in R. Koch, G. Rodosek (eds), Procedings of the 15th Conference on Cyber Warfare and Security, Munich, July, 2016. ISBN1910810932, 9781910810934.

Mari Malvenishv, "Role and Objectives of the Cybersecurity Bureau". Online Presentation by the Cybersecurity Bureau of Georgia, 2015. Available at: www./slideplayer.com/slide/9759466/

Sarma, Sanghamitra. "Cyber Security Mechanism in European Union." (2016).

Т4-В3: Киберкриминалистика

Описание

Киберкриминалистика – это приложение методов расследования и анализа для сбора, использования и сохранения цифровых доказательств. Данная сфера включает в себя цифровую криминалистику, криминалистику аппаратных средств и криминалистику человеческого фактора. Хотя криминалистическая экспертиза представляет приоритетную значимость для осуществляемого в рабочем порядке системного сопровождения и повышения эффективности проводимых операций, для целей формирования доказательственных материалов в ходе уголовных расследований необходим более жесткий контроль такого рода деятельности. В заключение следует отметить, что хорошо зарекомендовавшие себя криминалистические технологии обеспечивают важные инструменты для понимания того, как противник пытается незаконным образом внедриться в действующие системы, например, путем раскрытия методов получения доступа к узлам командования и управления войсками или разработки хакерских программ.

В настоящем разделе рассматриваются основные вызовы в области криминалистики, связанные с контролем и ликвидацией последствий «киберинцидентов». Криминалистические технологии можно применять при расследовании такого рода инцидентов, сборе разведданных и организации уголовного преследования с привлечением органов правопорядка. В материале описаны инструменты и методы получения информации из разных источников, анализа информации и воспроизведения последовательности событий. Эти инструменты и методы можно использовать для построения схемы установления «авторства», либо для проработки разных схем последующих шагов, начиная с отслеживания и мониторинга действий и заканчивая возбуждением уголовного дела против виновных лиц. Кроме того, слушатели узнают о порядке сбора и анализа тактико-криминалистических данных по финансовым правонарушениям, в частности, по отмыванию денег.

Участники программы познакомятся с проблемами, связанными со сбором тактико-криминалистических данных из разных источников, в том числе компьютеров, сетей, мобильных, сенсорных устройств и БД.

Результаты обучения

Слушатели продемонстрируют понимание:

- вопросов, связанных со сбором тактико-криминалистических данных из разных источников, в том числе компьютеров, сетей, мобильных, сенсорных устройств и БД;
- важности анализа тактико-криминалистических данных для целей воспроизведения последовательности событий инцидентов и установления «авторства»; а также
- действующего на национальном уровне законодательства и нормативных положений, регулирующих порядок сбора данных для информационного сопровождения осуществляемых органами правопорядка действий.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

- Создание устойчивой системы для обеспечения восстановления нормальной работы после киберинцидента
- Криминалистическая экспертиза элементов социального инжиниринга, используемых для получения доступа к системам
- Представляющие ценность для криминалистики аппаратные средства
- Использование результатов криминалистической экспертизы для уголовного преследования
- Автоматизированные средства для использования основополагающих методов криминалистики в оперативно-розыскных целях

Методика обучения /оценка результатов

Преподавание организовано в форме лекций, демонстрации материала и обсуждений конкретных примеров, иллюстрирующих различные элементы криминалистики.

Схема аттестации разрабатывается с учетом уровня знаний и освоения материала, соответствующего разработанному на основе настоящего базового учебного плана курсу.

Оценка знаний проводится в устной и письменной форме.

Учебные и справочные материалы

Сантош Бабу и С. Мани Мегалай. Криминалистическая экспертиза по фактам киберинцидентов и анализ среды облачной обработки данных. Международный журнал информатики и компьютерной технологии Б: облачные и распределенные технологии 15. Выпуск

1. – Редакция 1. 2015. https://globaljournals.org/GJCST_Volume15/1-Cyber-Forensic-Investigation.pdf

Ибрагим Баггили и Фрэнк Бретингер. Научно-образовательная лаборатория киберкриминалистики при Университете Нью-Хейвена. Источники данных для оптимизации киберкриминалистики – что может предложить мир социальных сетей. Документы весеннего симпозиума AAAI 2015 г. Пало Альто, Стэнфордский университет. – Март 2015 г. http://www.researchgate.net/profile/Ibrahim_Baggili/publication/274065229_Data_Sources_for_Advancing_Cyber_Forensics_What_the_Social_World_Has_to_Offer/links/55134a630cf283ee0833818c.pdf

Risto Vaarandi, Paweł Niziński, NATO Cooperative, Cyber Defence Centre of Excellence, Tallinn, Estonia. 2013 "A Comparative Analysis of Open-Source Log Management Solutions for Security Monitoring and Network Forensics". Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/VaarandiNizinski2013_Open-SourceLogManagementSolutions.pdf

Xiuzhen Cheng, Miroslaw Kutyłowski, Kuai Xu, Haojin Zhu, "Special Issue on Cybersecurity, Crime, and Forensics of Wireless Networks and Applications." Security and Communications Networks. Vol.8, Issue 17. 2015. Journal ISSN:1939-0122.

Åuteva Natal¡a, Mileva Aleksandra; Loleski Mario, "Finding Forensic Evidence for Several Web Attacks", International Journal of Internet Technology and Secured Transactions, Vol6., No.1, 2015. Journal ISSN: 1748-5703.

Akinola Ajijola, Pavol Zavarsky, Ron Ruhl, "A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012". Paper presented at the 'World Congress on Internet Security (WorldCon)' 2014. pp66-73. 10.1109/WorldCIS.2014.7028169. Available from the IEEE at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7028169&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7028169

Choi, Yangseo, Joo-Young Lee, Sunoh Choi, Jong-Hyun Kim, and Ikkyun Kim. "Introduction to a network forensics system for cyber incidents analysis." In 2016 18th International Conference on Advanced Communication Technology (ICACT), pp. 50-55. IEEE, 2016.

T4-B4: Аудит и оценка безопасности на национальном уровне

Описание

Оценка готовности в сфере безопасности – важная для государства функция. Такого рода оценка помогает проверить работу контрольных механизмов и выявить пробелы в инфраструктуре и политике безопасности. Оценку безопасности можно проводить на разных уровнях. Сначала можно протестировать отдельные механизмы контроля безопасности с помощью инструментов аудита. Затем с помощью организации учений и моделирования обстановки в режиме реального времени осуществляется комплексная оценка - на общесистемном или организационном уровне. В данном разделе приводится общая информация об инструментах и процессах аудита и оценки безопасности, на основании которой слушатели познакомятся с методами выявления и взвешивания оценки остаточной уязвимости систем; более того, эти механизмы оценки и контроля помогают определить порядок анализа готовности киберсистем для взаимодействия с конкретными категориями известных субъектов угрозы и спланировать меры на случай возникновения неизвестной угрозы (это так называемые угрозы «нулевого дня», при которых отсутствует предупреждение о конкретных средствах нападения или хакерских действиях).

Физические лица и организации используют самые разные инструменты и методы повышения самобдительности, начиная от анкет-опросников до технических средств. Освещаемые в настоящем разделе материалы призваны расширить понимание роли самобдительности применительно к кибербезопасности граждан и корпоративных субъектов. Анализ сильных и слабых сторон различных инструментов и подходов важен для понимания их ценности. Проводимая на постоянной основе самооценка может снизить риски. Для действенной самооценки также важно учитывать потенциальные субъективные факторы. Перевод результатов в оперативную плоскость – необходимый элемент любой самооценки. Поскольку уровень безопасности связан со значением, важностью или конфиденциальностью объекта безопасности, универсально применимой и приемлемой модели не существует. Скорее, желаемая степень кибербезопасности будет определяться выбранными стандартами и уровнем результативности, достижение которого необходимо обеспечить.

Результаты обучения

Слушатели:

- будут понимать важность инструментов аудита и оценки безопасности, а также
- научатся оценивать и применять на практике соответствующие инструменты самооценки с учетом национальной специфики.

Вопросы и подходы, которые в перспективе могут быть включены в учебные блоки

Вот некоторые темы для проработки:

- передовой опыт организаций, которые используют методы самооценки
- обсуждение конкретных примеров ситуаций, в которых самобдительность послужила делу укрепления безопасности

Методика обучения /оценка результатов

Слушатели практикуются в использовании действующих на национальном уровне средств самооценки – если таковые существуют; если их нет, можно применить Инструмент оценки кибербезопасности (CSET) Управления внутренней безопасности США (УВБ) или его аналог. Целесообразно провести сравнительный анализ национальных методов и метода УВБ США.

Схема оценки разрабатывается с учетом уровня знаний и освоения материала, соответствующего разработанным на основе настоящего базового учебного плана курсам.

Учебные и справочные материалы

Институт проблем повышения устойчивости функционирования предприятий. Руководство по передовой практике за 2013 г. – глобальное издание: методическое руководство по международной передовой практике в области повышения устойчивости функционирования предприятий и организаций (Англия), 2013. www.thebci.org/index.php/resources/the-good-practice-guidelines

Международный совет по стандартам аудита и подтверждения. Стандарт ISAE 3402 «Отчетность и контроль в организациях сферы услуг». http://isae3402.com/ISAE3402_overview.html

Международная организация по стандартизации/ Международная электротехническая комиссия. *ISO/ IEC 15408*: общие критерии для оценки безопасности информационных технологий, версия 3.1, ред. 4, CCMB-2012-09-001. - Сентябрь 2012. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

Кит Стуффер, Джо Фалько и Карен Скарфоне. Специальная публикация *NIST 800-82: методическое руководство по безопасности систем управления производственными процессами*. Национальный институт стандартов и технологий Министерства торговли США, июнь 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

Управление внутренней безопасности США. Обзор потенциала восстановления нормального функционирования киберсистем (ОПВК) – набор инструментов самооценки. Университет Карнеги-Меллон, февраль 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf

Управление внутренней безопасности США. Обзор потенциала восстановления нормального функционирования киберсистем (ОПВК) – вопрос по методическим указаниям. Университет Карнеги-Меллон, февраль 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

Ivan Alcoforado, “Leveraging Industry Standards to Address Industrial Cybersecurity Risk”, ISACA Journal, Vol 6, 2014; Journal ISSN: 1944-1967.

Stefan Laube, Rainer Böhme (Department of Information Systems, University of Munster, Germany; Institute of Computer Science, University of Innsbruck, Austria), “The Economics of Mandatory Security Breach Reporting to Authorities”. Available at: http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_laube.pdf

Yulia Cherdantseva, et al. “A Review of Cyber Security Risk Assessment Methods for SCADA systems.” Electronic monograph. Available at the British Library, reference: UIN: ETOCvdc_100030733535.0x000001.

Abhijit Gupta, Subarna Shakya, “Information System Audit; A study for security and Challenges in Nepal”, in, International Journal of Computer Science and Information Security, Vol.13, No. 11 (Nov 2015) pp 1-4. Journal ISSN 1947-5500.

Karabacak, Bilge, Sevgi Ozkan Yildirim, and Nazife Baykal. “Regulatory approaches for cyber security of critical infrastructures: The case of Turkey.” Computer Law & Security Review 32, no. 3 (2016): 526-539.

Список сокращений

APT advanced persistent threat
целенаправленная устойчивая угроза

AS autonomous system (discrete subdivision of the Internet)
автономная система (отдельный элемент Интернета)

ASN autonomous system number
номер в автономной системе

BGP Border Gateway Protocol
протокол BGP

BSA basic security architecture
базовая архитектура системы защиты

BYOD Bring Your Own Device
концепция использования собственных устройств

CERT cyber emergency response team
Группа реагирования на ЧС в киберпространстве

COBIT Control Objectives for Information and Related Technology
контрольные задачи для информационных и связанных с ними технологий

COMSEC communications security
безопасность связи

CSET Cyber Security Evaluation Tool
инструмент для оценки кибербезопасности

CSET Cyber Security Evaluation Tool
инструмент для оценки кибербезопасности

DDoS Distributed Denial of Service
распределенное кибернападение типа «отказ в обслуживании»

DHS U.S. Department of Homeland Security
Управление внутренней безопасности США

DNS domain name system
доменная система имен

DoS Denial of Service
отказ в обслуживании

ENISA European Agency for Network and Information Security
Европейское агентство по безопасности сетей и информации

ESCWG Emerging Security Challenges Working Group
Рабочая группа «Формирующиеся вызовы в сфере безопасности»

FTP File Transfer Protocol
протокол передачи файлов

HTTP Hypertext Transfer Protocol
протокол переноса гипертекста

HTTPS Secure Hypertext Transfer Protocol
защищенный протокол переноса гипертекста

IANA Internet Assigned Numbers Authority
Управление по присвоению интернет-номеров

ICANN Internet Corporation for Assigned Names and Numbers
Интернет-корпорация по присвоенным именам и номерам

ICS industrial control system
система управления производственными процессами

ICT information and communications technology
информационно-коммуникационные технологии

IDS intrusion detection system
система обнаружения сетевых атак

IGF Internet Governance Forum
Форум по управлению использованием Интернета

IP Internet Protocol
интернет-протокол

IS information security
безопасность информации

ISACA	Information Systems Audit and Control Association Ассоциация аудита и контроля информационных систем
ISO	International Organization for Standardization Международная организация по стандартизации
ISP	Internet service provider провайдер интернет-услуг
IT	information technology информационные технологии
ITU	International Telecommunications Union Международный союз электросвязи
LAN	local area network локальная сеть
NIR	National Internet Registry Национальный интернет-регистратор
NIST	(U.S.) National Institute of Standards and Technology Национальный институт США по стандартам и технологиям
PfPC	Partnership for Peace Consortium Консорциум «Партнерство ради мира»
PIT system	platform IT system платформная ИТ-система
RACI	Responsibility, Accountability, Command and Information ответственность, подотчетность, управление и информация
SCADA	Supervisory Control and Data Acquisition система оперативно-диспетчерского управления
SCRM	supply chain risk management управление рисками логистической цепи
SFTP	Secure File Transfer Protocol защищенный протокол передачи файлов
SIEM	security information and event management организация данных и мероприятий в сфере безопасности
SME	subject matter expert специалист профильного направления
SMTP	Simple Mail Transfer Protocol протокол простой электронной передачи
SQL	Structured Query Language Международный стандартный язык для определения и доступа к реляционным базам данных
SSH	Secure Shell протокол безопасной оболочки
SSL	Secure Socket Layer протокол защищенных сокетов
TCP	Transmission Control Protocol протокол управления передачей данных
TRA model	Threat and Risk Assessment model модель оценки угроз и рисков
UNIDIR	United Nations Institute for Disarmament Research Институт ООН по исследованию проблем разоружения

Словарь специальных терминов

Примечание: не все приведенные ниже термины упоминаются в тексте материала, но многие из них можно с пользой применить при разработке конкретных практических заданий и пр.

A

access control mechanism
механизм контроля доступа. Определение: меры безопасности, осуществляемые с целью обнаружения и предотвращения несанкционированного доступа, а также обеспечения санкционированного доступа к информационной системе или на физический объект.

active attack
активная атака. Определение: фактическая атака, совершаемая источником намеренной угрозы с целью изменить систему, системные ресурсы, хранящиеся в ней данные или ее режим работы.

advanced persistent threat(s)
целенаправленная устойчивая угроза (угрозы). Определение: противник, обладающий высоким уровнем профессиональных знаний и значительными по объему ресурсами, которые обеспечивают для него возможности достижения поставленных целей за счет организации многовекторной атаки (напр., кибер-, физического нападения и введения в заблуждение). Источник: NIST SP 800-53, ред. 4.

antivirus software
антивирусное ПО. Определение: программа, осуществляющая мониторинг ПК или сети для обнаружения или определения основных категорий вредоносных кодов, а также для предотвращения или локализации хакерских инцидентов, в ряде случае – за счет ликвидации или нейтрализации вредоносного кода.

attack
атака. Определение: попытка получить несанкционированный доступ к системным сервисам, ресурсам или информации, либо попытка нарушить целостность системы.

attack pattern
алгоритм атаки. Определение: аналогичные киберинциденты или действия, указывающие на то, что атака была совершена или совершается, в результате чего имеет место нарушение режима безопасности – фактическое или потенциальное.

attack signature
«почерк» хакера. Определение: отличительная черта или отчетливый сценарий развития событий, который можно отследить или использовать при сопоставлении инцидента с выявленными ранее атаками.

attack surface
вид атаки. Определение: набор методов, с помощью которых противник может внедриться в систему и потенциально нанести ущерб. Расширенное определение: отличительные черты системы, позволяющие противнику внедриться в систему, атаковать ее или сохранять в ней свое присутствие. Адаптированный вариант: Манадхата П.К. и Уинг, Дж. М. Оценка видов атак. http://www.cs.cmu.edu/~pratyus/as.html#introduction.

authentication
проверка прав доступа. Определение: процесс установления личности или других атрибутов субъекта (пользователя, процесса или устройства). Расширенное определение: также процесс установления источника и целостности данных.

B

botnet
бот-сеть. Определение: комплекс ПК, зараженных зловредным кодом и управляемых в пределах сети.

Build Security
построение системы безопасности. Определение: набор принципов, методов и инструментов, используемых для проектирования, разработки и оптимизации информационных систем и ПО, которые повышают устойчивость к уязвимостям, «брешам» и атакам.

C

capability
потенциал. Определение: средства для выполнения задачи, функции или цели.

cloud computing
облачная обработка данных. Определение: схема запуска осуществляемого по требованию сетевого доступа к коллективному пулу конфигурируемых вычислительных возможностей или ресурсов (т.е. сетей, серверов, блоков хранения данных, приложений и сервисов), которую можно оперативно настроить и внедрить при минимальных организационных усилиях или вмешательстве со стороны провайдера сервиса.

Computer Network Defense Analysis
Анализ защиты компьютерной сети. Определение: использование мер защиты и информации, собранной из разных источников, для выявления, анализа и доведения до сведения инцидентов, которые имеют или могут иметь место внутри сети, с целью защиты информации, информационных систем и сетей от угроз.

critical infrastructure
важнейшие объекты инфраструктуры. Определение: системы и активы (физические или виртуальные), которые имеют для общества настолько большое значение, что нарушение их функционирования или разрушение может оказать дестабилизирующее воздействие на безопасность, защиту населения, экономику, здравоохранение, окружающую среду или сразу на несколько этих параметров.

cryptography
криптография. Определение: использование математических методов для оказания услуг в сфере безопасности, например, в плане обеспечения конфиденциальности, целостности данных, аутентификации субъектов и происхождения данных.

cyber ecosystem
киберэкосистема. Определение: взаимосвязанная информационная инфраструктура или взаимодействие людей, процессов, данных и информационно-коммуникационных технологий в определенной среде или условиях, которые влияют на такого рода взаимодействие.

cybersecurity
кибербезопасность. Краткое определение: деятельность или процесс, способность, потенциал или состояние, при котором информационно-коммуникационные системы и содержащаяся в них информация ограждены и (или) защищены от ущерба, несанкционированного применения, модификации или вторжения. Расширенное определение: стратегия, политика и стандарты, регулирующие безопасность киберпространства и осуществляемых в нем операций и включающие в себя комплексную систему мер политики и мероприятий по снижению угрозы, уязвимости, сдерживанию, обеспечению международного взаимодействия, реагированию на инциденты, оптимизации потенциала для восстановления нормальной жизнедеятельности, включая проведение информационно-сетевых операций, обеспечение доступности, целостности и безопасности информации, реализацию правоохранительных и дипломатических мер, выполнение военных и разведывательных задач в части, относящейся к безопасности и стабильности глобальной инфраструктуры информации и средств связи. Определение адаптировано из материалов CNSSI 4009, NIST SP 800-53 ред. 4, NIPP, Установленная УВБ цель по обеспечению готовности; Обзор политики в киберпространстве – Белый дом, май 2009.

cyberspace
киберпространство. Определение: электронно-цифровой мир, созданный взаимосвязанными сетями информационных технологий и размещаемой в этих сетях информацией.

D

data mining
извлечение информации из данных. Определение: процесс или методы, используемые для анализа крупных массивов существующей информации для выявления ранее не установленных схем или корреляций.

denial of service
отказ в обслуживании. Определение: атака, которая предотвращает или препятствует санкционированному использованию ресурсов или сервисов информационной системы.

digital forensics
цифровая криминалистика. Определение: процессы и специальные методы сбора, сохранения и анализа связанных с системами данных (цифровых доказательств) для проведения оперативно-следственных мероприятий.

digital rights management
управление цифровыми правами. Определение: форма технологии контроля доступа для защиты и управления использованием цифрового контента или устройств в соответствии с тем, как это было задумано провайдером контента (устройства).

distributed denial of service
распределенная атака типа «отказ в обслуживании». Определение: метод отказа в обслуживании, который предполагает использование целого ряда систем для организации атаки в синхронном режиме.

E

enterprise risk management
управление рисками предприятия. Определение: комплексный подход к управлению рисками, который предусматривает подключение кадровых ресурсов, процессов и систем в масштабах всей организации для оптимизации механизмов принятия решений по управленческим рискам, которые могут снизить потенциал организации в плане выполнения поставленных задач.

exploit
компьютерное вторжение. Определение: метод преодоления системы безопасности сети или информационной системы в нарушение политики безопасности.

F

firewall
межсетевая защита. Определение: возможность сокращения трафика между сетями и (или) информационными системами.

H

hacker
хакер. Определение: не имеющий полномочий доступа пользователь, который пытается получить или получает доступ к информационной системе.

I

ICT supply chain threat
угроза для логистической цепочки ИКС. Определение: антропогенная угроза, создаваемая в результате несанкционированного использования логистической цепочки системы ИКТ, включая процессы закупок.

inside(r) threat
инсайдерская угроза. Определение: лицо или группа лиц в организации, которые представляют собой потенциальный риск за счет нарушения политики безопасности. Расширенное определение: отдельное лицо или группа лиц, обладающих доступом и (или) инсайдерскими знаниями компании, организации или предприятия, которые обеспечивают для них возможность использовать уязвимые места безопасности, систем, услуг, продуктов или объектов указанной структуры с целью нанесения ущерба.

integrated risk management
комплексное управление рисками. Определение: структурированный подход, обеспечивающий для предприятия или организации возможность обмениваться информацией о существующих рисках и результатах анализа рисков, а также синхронизировать автономные, но в то же время дополняющие друг друга стратегии управления рисками с целью объединения усилий в масштабах всей организационной структуры.

intrusion
вторжение. Определение: несанкционированный акт, совершаемый с целью обойти механизмы безопасности сети или информационной системы.

intrusion detection
выявление вторжения. Определение: процесс и методы анализа информации из сетей и информационных систем с целью установления фактов проникновения в систему безопасности или нарушения действующего режима безопасности.

K

keylogger
программа «взломщик». Определение: ПО или аппаратные средства, которые отслеживают нажатие клавиш и использование клавиатуры, как правило, негласно (тайно), с целью мониторинга действий пользователя информационной системы.

M

malicious code
вредоносный код. Определение: код программы, используемый с целью выполнения несанкционированной функции или процесса, которые оказывают негативное воздействие на режим конфиденциальности, целостность или доступность информационной системы.

malware
вредоносное программное средство. Определение: ПО, нарушающее работу системы за счет выполнения несанкционированной функции или процесса.

N

network resilience
устойчивость сети. Определение: способность сети (1) функционировать в непрерывном режиме (т.е. обладать высокой устойчивостью на случай сбоев и способностью функционировать в неполном режиме при нарушении работы); (2) восстанавливаться при отказе в работе, а также (3) масштабироваться для обеспечения оперативно возникающих или непредсказуемых потребностей.

non-repudiation
предотвращение отказа. Определение: свойство, достигаемое за счет применения методов шифрования и имеющее целью обеспечить защиту от физического или корпоративного лица, ложно отрицающего факт совершения конкретного действия, связанного с данными. Расширенное определение: обеспечение возможности установить факт совершения отдельным лицом конкретного действия, в частности, создания данных, отправки (получения) сообщения или утверждения информации.

P

passive attack
пассивная атака. Определение: фактическое нападение, совершаемое источником международной угрозы, который пытается получить или использовать информацию, содержащуюся в системе, но при этом не пытается изменить саму систему, ее ресурсы, сохраняемые в ней данные или режим функционирования.

phishing
«фишинг». Определение: цифровая форма социального инжиниринга, используемая с целью ввести объект в заблуждение для получения от него закрытой для доступа информации.

R

redundancy
резервирование. Определение: дополнительные или альтернативные системы, подсистемы, объекты или процессы, которые в случае утраты или нарушения работы другой системы, подсистемы, объекта или процесса поддерживают параметры функционирования на соответствующем уровне.

resilience
устойчивость. Определение: способность адаптироваться к изменяющимся условиям, а также обеспечивать готовность к сбоям, противостоять им и оперативно восстанавливать нормальный режим работы.

risk analysis
анализ рисков. Определение: систематическое рассмотрение компонентов и характеристик рисков.

risk assessment
оценка рисков. Определение: продукт или процесс, который собирает информацию и присваивает значения переменных величин рискам для получения информации, используемой для определения приоритетов и принятия решений, разработки или сравнения планов действий. Расширенное определение: оценка рисков, угрожающих субъекту, объекту, системе или сети, деятельности организации, физическим лицам, географической области, другим организациям или обществу, включая определение того, в каком объеме негативные обстоятельства или события могут повлечь за собой пагубные последствия.

risk management
управление рисками. Определение: процесс определения, анализа, оценки и передачи риска, а также его принятия, предотвращения, переноса или контроля на приемлемом уровне с учетом связанных с принимаемыми мерами затрат и преимуществ. Расширенное определение включает в себя: (1) проведение оценки рисков; (2) реализацию стратегий для снижения рисков; (3) мониторинг рисков на постоянной основе в течение длительного времени, а также (4) документирование комплексной программы управления рисками.

S

spam
спам. Определение: нецелевое использование системы передачи электронных сообщений для бессистемной массовой рассылки несогласованных с получателем сообщений.

spoofing
«спуфинг». Определение: фальсифицирование адреса, с которого отправляется сообщение, для получения нелегального (несанкционированного) доступа к защищенной системе.

spyware
шпионское ПО. Определение: ПО, тайно или негласно устанавливаемое в информационной системе без ведома пользователя или владельца системы.

Supervisory Control and Data Acquisition (SCADA)
дистанционное управление и сбор данных. Определение: общий термин, используемый для обозначения автоматизированной системы, способной обеспечивать сбор и обработку данных и применение механизмов функционального контроля над территориально распределенными объектами на значительных расстояниях.

supply chain
цепочка поставок. Определение: система организаций, людей, деятельности, информации и ресурсов, обеспечивающая перемещение продуктов, включая компоненты продуктов и (или) услуг от поставщиков до заказчиков.

supply chain risk management
управление рисками цепочки поставки. Определение: процесс выявления, анализа и оценки рисков цепочки поставок, а также их принятия, предотвращения, перевода или контроля в соответствующем объеме с учетом связанных с принимаемыми мерами затрат и преимуществ.

T

threat
угроза. Определение: обстоятельство или событие, которая обладает или свидетельствует о наличии потенциала в части использования уязвимых мест и оказания негативного воздействия (создания неблагоприятных последствий) на деятельность организаций и имеющиеся у них активы (включая информацию и информационные системы), физических лиц, прочие учреждения или общество.

threat actor/agent
злоумышленник/фактор угрозы. Определение: лицо, группа лиц, организация или правительство, осуществляющие или имеющие намерение осуществлять злоумышленные действия.

threat assessment
оценка угрозы. Определение: продукт или процесс выявления или оценки субъектов, действий или событий, происходящих самопроизвольно или возникающих в результате деятельности человека, которые имеют или свидетельствуют о наличии потенциала в части причинения ущерба жизни, информации, деятельности и (или) имуществу.

threat vector
вектор угрозы. Определение: средства включения угрозы в задачу или подход, реализуемые для актуализации угрозы.

Trojan horse
«Троянский конь». Определение: компьютерная программа, которая на первый взгляд выполняет нужную функцию, но наряду с этим обладает скрытым и потенциально вредоносным функционалом, действующим в обход механизмов безопасности, в ряде случае за счет использования легитимных авторизаций системного объекта, который инициирует программу.

U

unauthorized access
несанкционированный доступ. Определение: любой доступ, который нарушает действующую политику безопасности.

V

virus
вирус. Определение: способная к саморепликации компьютерная программа, которая может «заразить» ПК – без разрешения или ведома пользователя – и затем распространить (тиражировать) вирус на другой ПК.

vulnerability
уязвимость. Определение: характеристика или конкретное слабое звено, из-за наличия которого организация или актив (например, информация или информационная система) может стать объектом для конкретной угрозы или характеризоваться уязвимостью к конкретному риску.

W

worm
вирус-червь. Определение: самореплицирующаяся, самораспространяющаяся автономная программа, которая тиражирует себя с использованием сетевых механизмов.

Z

Zero-day exploit
атака «нулевого дня». Определение: атака, при которой удар – который наносится без предупреждения и устаналивается в процессе его нанесения – поражает невыявленное уязвимое звено.

Материал адаптирован из научного глоссария «Кибербезопасность» УВБ США и дополнен.

Руководители и редакторы: Шон Костиган и Майкл Хеннесси
Члены группы по разработке учебной программы и консультанты

Фамилия, имя, отчество	**Страна**	**Место работы**	
Д-р Ата Аталай	Турция	Начальник управления Генеральный секретариат Совета национальной безопасности	
Г-жа Мария Авдеева	Менеджер	Международное развитие Харьковский национальный юридический университет	
Г-жа Александра Бильска	Консультант	Разведывательное управление Польша	
Г-н Джузеппе Конти	Италия	Технический директор Компания Trilogis	
Г-н Шон С. Костиган	США	Преподаватель Европейский центр по изучению вопросов безопасности им. Маршалла	
Г-н Жан д'Андуран	Франция	Координатор учебно-образовательных программ в области обороны Международный штаб НАТО	
П/п-к Дирк Дюбуа	Бельгия	Европейский коллеж безопасности и обороны	
Д-р Дэвид Эмелифеонву	Канада	Старший офицер отдела формирования л/с Департамента подготовки Штаба Министерство обороны	
Г-н Дэвид Франко	США	Старший оперуполномоченный Федеральное бюро расследований	

Д-р Петр Гавличек	Польша	Заместитель ректора по инновациям Университет национальной обороны	
Д-р Санджей Гоэл	США	Начальник научно-исследовательского отдела Центра информационной криминалистики и безопасности Университет штата Нью-Йорк Олбани	
Г-н Андриа Готсиридзе	Грузия	Начальник Управления кибербезопасности Министерство обороны	
Г-н Арман Григорян	Армения	Руководитель Группы по кибербезопасности Институт национальных стратегических исследований	
Д-р Майкл А. Хеннесси	Канада	Преподаватель, проректор по научной работе Королевский военный колледж	
Кап. 2 р. Андреас Хильденбранд	ФРГ	Преподаватель Центр по изучению вопросов безопасности им. Маршалла	
Д-р Динос Кериган-Кироу	Великобритания	Преподаватель кафедры информатики и математики Гринвичский университет	UNIVERSITY of GREENWICH
Д-р Скотт Найт	Канада	Преподаватель, зав. кафедрой информатики и электротехники Королевский военный колледж	
Г-н Фредерик Лабарр	Канада	Руководитель программы Консорциум «Партнерство ради мира»	
Г-н Филип Ларк	США	Руководитель программы «Кибербезопасность» Центр по изучению вопросов безопасности им. Маршалла	

Д-р Густав Линдстрем	Швеция	Руководитель программы «Формирующиеся вызовы в сфере безопасности» Женевский центр политики безопасности	GCSP
Д-р Вахтанг Маизая	Грузия	Преподаватель программы магистратуры по специальности «международная безопасность» Кавказский международный университет	
Д-р Петар Моллов	Болгария	Доцент Институт перспективных оборонных исследований	
Г-н Крис Палларис	Великобритания	Директор Компания i-intelligence	i-INTELLIGENCE
Г-н Даниэл Педер Багге	Чешская Республика	Специалист в области кибербезопасности/политики Управление национальной безопасности	NBU
Г-н Рафаэль Перл	США	Директор Консорциум «Партнерство ради мира»	
Г-жа Мака Петриашвили	Грузия	Начальник Управления кадров Министерство обороны	
Г-жа Стела Петрова	Болгария	Консультант Сеть «Европейское лидерство»	European Leadership Network
Д-р Беньямин Погосян	Армения	Зам. директора Институт национальных стратегических исследований	
Г-н Олександр Потил	Украина	Преподаватель дисциплины «безопасность ИТ» Харьковский университет ВВС	

Д-р Детлеф Пуль	ФРГ	Старший консультант Управление НАТО по анализу формирующихся вызовов в сфере безопасности	
Г-н Нил Робинсон	Великобритания	Старший научный сотрудник Корпорация «РЭНД» (Европа)	
Г-н Гиги Роман	Румыния	АДЛ Школа НАТО в Обераммергау, ФРГ	
П/п-к Генадие Сафонов	Молдова	Управление связи и информатики Академия обороны Молдовы	
Г-н Данило Шевченко	Украина	Руководитель проекта Центр стратегических исследований и инноваций	
Г-жа Наталья Спину	Молдова	Директор Центр кибербезопасности при Государственной канцелярии	
Д-р Алан Дж. Столберг	США	Координатор учебных программ в области обороны Корпорация «РЭНД»	
Д-р Тодор Тагарев	Болгария	Преподаватель/руководитель Управление «ИТ для безопасности» и Центр контроля безопасности и обороны	
Д-р Рональд Тэйлор	США	Президент Центр стратегического руководства в сложных условиях	
Г-н Богдан Удристе	Румыния	Специалист в области безопасности информационных систем Миссия ЕС по мониторингу	
Г-н Джозеф Ванн	США	Преподаватель Европейский центр по изучению вопросов безопасности им. Маршалла	

Редакционная коллегия и распространение материала

Редакторы:

Шон С. Костиган
Преподаватель
Европейский центр по изучению вопросов безопасности им. Джорджа К. Маршалла
Sean S. Costigan
George C. Marshall European Security Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
sean.costigan@pfp-consortium.org

Д-р Майкл А. Хеннесси
Профессор истории и военных
исследований Королевского военного
колледжа Канады:
Michael A. Hennessy, PhD
Royal Military College of Canada
P.O. Box 17000 STN FORCES
Kingston, ON Canada
K7K 7B4
Hennessy-m@rmc.ca

Метранпаж / Распространение материала:

Габриелла Лурвиг-Жандарм
Gabriella Lurwig-Gendarme
NATO International Staff
lurwig.gabriella@hq.nato.int

1217-16 NATO Graphics & Printing — ISBN 978-92-845-0196-0