Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Герман Капониг, *Connections QJ* 19, № 1 (2020): 21-41
https://doi.org/10.11610/Connections.rus.19.1.03

Национальная политика кибербезопасности

Национальная политика кибербезопасности и обороны Австрии: вызовы и путь вперед

Генерал-майор Герман Капониг

Центр ИКТ и кибербезопасности, Вооруженные силы Австрии

Резюме: В статье представлена политика кибербезопасности Австрии в рамках общегосударственного контекста. Это комплексная, интегрированная, проактивная и основанная на солидарности и сотрудничестве в рамках и вне рамок Европейского союза политика. Ожидается, что прозрачное управление, сотрудничество между публичными агентствами, бизнесом, исследовательскими институтами и гражданами, инвестиции в готовность, исследования и разработки будут эффективно защищать жизненно важную информацию и критическую инфраструктуру. Министерство обороны и австрийские вооруженные силы дают свой вклад в национальную политику в основном через работу Совместного командования сил, Командования коммуникационных и информационных систем и кибероборонны и двух разведывательных служб.

Ключевые слова: кибероборона, критическая инфраструктура, общегосударственный, межведомственное сотрудничество, платформа по кибербезопасности.

Основные моменты политики: национальная военная политика кибербезопасности Австрии в рамках общегосударственного контекста

«Австрийская стратегия безопасности: Безопасность для нового десятилетия – формирование безопасности», была принята Национальным советом

Австрии в 2013 году (АСБ 2013).[1] За ней в том же году последовала «Австрийская стратегия кибербезопасности» (АСКБ 2013),[2] которая была разработана в соответствии с АСБ. Оба документа были разработаны на национальном уровне.

АСБ 2013 обрисовывает новые вызовы, риски и угрозы, в том числе и киберугрозы (атаки против безопасности ИТ систем, или «кибератаки») на основе анализа австрийской среды безопасности. Кроме того, АСБ 2013 делает отличие между двумя ключевыми областями в терминах требуемой разработки политики.

В главе «Политика безопасности на национальном уровне: *внутренняя безопасность*» рассматриваются киберпреступления, кибератаки и злонамеренное использование Интернета в экстремистских целях, а также сетевая безопасность, являющиеся новыми и специфическими вызовами для всех затрагиваемых игроков. Кроме того, в этой главе обращается внимание на то, что требуется *широкое сотрудничество, основанное на комплексной концепции*. В той же главе, под заголовком *«Политика обороны»* постулируется, что управление суб-конвенциональными угрозами и новыми опасностями, проистекающими из кибератак, может создать новую сферу военной деятельности. Из этих двух пунктов можно сделать вывод, что АСБ идентифицирует современные киберугрозы, но не занимается четко расписанными контрмерами.

От вооруженных сил требуется расширить свои кибер способности в соответствие с национальной концепцией кибербезопасности. Это означает, что вооруженные силы должны быть в состоянии обеспечивать кибер поддержку и содействие, сравнимые с военным содействием в случае оказания помощи при бедствиях.

3 июля 2013 года Национальный совет принял резолюцию, требующую от Федерального правительства Австрии разработать политику безопасности Австрии в соответствии с определенными основными принципами. В отношение кибербезопасности в резолюции сказано:

> Угрозы, порожденные государственными и не-государственными акторами в киберпространстве, постоянно увеличиваются. Вот почему кибербезопасность становится все более важной. Меры по повышению безопасности компьютерных систем, а также безопасности Интернета, следует интенсифицировать.

Австрийская стратегия кибербезопасности от 2013 года должна осуществляться и обновляться регулярно в соответствии с текущим развитием событий. Это означает, что АСКБ 2013 должна осуществляться на нацио-

[1] "Österreichische Sicherheitsstrategie: Sicherheit in einer neuen Dekade – Sicherheit gestalten," Vienna, July 2013, https://www.bmi.gv.at/502/files/130717_Sicherheitsstrategie_Kern_A4_WEB_barrierefrei.pdf.

[2] "Austrian Cyber Security Strategy," Vienna, 2013, https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf.

нальном уровне и развиваться дальше. В настоящее время разрабатываются национальные планы для АСКБ 2.0 – которая будет основываться на уже достигнутых целях, а также на развитие событий и требований, которые произошли с тех пор.

В введении в АСКБ 2013 объяснено, что атаки из киберпространства являются непосредственной угрозой для безопасности и нормального функционирования государства, экономики, науки и общества. Они могут иметь существенное отрицательное влияние на нашу повседневную жизнь. Такие негосударственные акторы, как преступники, организованная преступность или террористы, а также такие государственные акторы, как секретные службы и вооруженные силы, могут использовать злонамеренно киберпространство в свои целях и оказывать влияние на его нормальное функционирование. Варианты угроз в киберпространстве и их использования практически бесконечны. Поэтому, *одним из главных приоритетов Австрии является работа по обеспечению безопасности киберпространства на национальном и международном уровнях*. Кибербезопасность означает безопасность инфраструктуры киберпространства, безопасность обмена данными в киберпространстве, и прежде всего, защита людей, использующих киберпространство.

Это общая, центральная задача государства, экономики и общества – обеспечить кибербезопасность в национальном и международном плане. АСКБ 2013 является комплексной и проактивной концепцией защиты киберпространства и людей в киберпространстве, одновременно с этим гарантируя соблюдение человеческих прав. Ожидается, что стратегия будет способствовать безопасности и устойчивости инфраструктур и услуг в киберпространстве. На первом месте, она создает готовность и уверенность в австрийском обществе.

В главе «Риски и угрозы» указывается, что киберпространство и безопасность людей в киберпространстве подвергаются ряду рисков и угроз, поскольку киберпространство также является полем преступной деятельности. Эти риски и угрозы занимают весь спектр от ошибок функционирования до массированных атак со стороны государственных акторов и не-государственных групп, использующих киберпространство в качестве оперативных форумов, не ограниченных национальными границами. *За этими атаками могут стоять и иностранные военные организации*.

Спектр рисков и угроз был представлен в особой Матрице кибер рисков (в действии с 2011).[3] Матрица рисков была пересмотрена и обновлена в 2016.[4] Киберпреступность, мошенничество с использованием личных данных, кибератаки или злонамеренное использование Интернета в экстре-

[3] "Cyber-Risikomatrix 2011," https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/KSO_Cyber_Risikomatrix.pdf, accessed March 12, 2020.

[4] "Cyber-Risikomatrix 2011."

мистских целях являются новыми серьезными проблемами, которые требуют широкого сотрудничества между правительственными и неправительственными организациями на национальном и международном уровне. Это является ясным указанием на то, что противодействие кибер-проблемам должно быть приоритетной задачей в национальной повестке дня, что нужно объединение всех сил в целостном общегосударственном подходе, и что национальное и международное сотрудничество очень важны.

Глава «Принципы» продолжается следующими определениями:

Современная политика кибербезопасности является сквозным вопросом, который оказывает влияние на многие сферы жизни и политики. Она должна разрабатываться с учетом комплексного и интегрированного подхода, должна позволять активное участие и должна реализовываться в духе солидарности.

Комплексная политика кибербезопасности означает, что внешняя и внутренняя безопасность, а также многие аспекты гражданской и военной безопасности, тесно переплетаются. Кибербезопасность выходит за круг ответственности традиционных ведомств безопасности и охватывает инструменты множества сфер политики.

Интегрированная политика кибербезопасности делает упор на разделение задач между государством, экономикой, академическими кругами и гражданским обществом. Она охватывает меры в следующих областях: политико-стратегическое управление, образование и квалификация, оценка рисков, профилактика и поддержка готовности, выявление и реакция, смягчение и восстановление, а также развитие государственных и не-государственных способностей и потенциалов. Интегрированная политика кибербезопасности должна основываться на кооперативном подходе на национальном и международном уровне.

Проактивная политика кибербезопасности означает, что предпринимаются меры для предотвращения угроз киберпространству и людям в киберпространстве, а также меры для смягчения последствий инцидентов (формирование безопасности).

Политика кибербезопасности, основанная на солидарности, учитывает, что из-за глобального характера киберпространства, кибербезопасность Австрии, ЕС и всего сообщества наций сильно взаимосвязаны. Обеспечение кибербезопасности требует интенсивного сотрудничества, базирующегося на солидарности на европейском и международном уровнях.

Основные вызовы политике Австрии и ключевые приоритетные области

На основании стратегических целей АСКБ 2013 обозначает семь областей действий и 15 мер:

- Область действий 1 – Структуры и процессы
- Область действий 2 – Управление

- Область действий 3 – Сотрудничество государства, экономики и общества
- Область действий 4 – Защита критической инфраструктуры
- Область действий 5 – Повышение готовности и квалификация
- Область действий 6 – Исследования и разработки
- Область действий 7 – Международное сотрудничество.

Сфера деятельности 1 – Структуры и процессы

Цель: В киберпространстве есть множество активных структур и игроков, которые работают по отдельности для обеспечения кибербезопасности. Несколько организаций, специализирующихся на кибербезопасности (например, Компьютерные команды реагирования на чрезвычайные ситуации, ККРЧС), уже играют важную роль в кибер кризисном менеджменте. Но общие процедуры кибербезопасности все еще официально не дефинированы. Поэтому необходимо определить процессы и структуры для целостной координации на политико-стратегическом и оперативном уровне путем подключения заинтересованных общественных и частных субъектов.

Меры:

1) Создание руководящих групп по кибербезопасности

В 2012 Совет министров Австрии сформировал *Руководящую группу по кибербезопасности*. Подчиняясь аппарату федерального канцлера, группа отвечает за координацию мер, связанных с кибербезопасностью на политико-стратегическом уровне, мониторингом и поддержкой реализации АСКБ 2013, за составление проекта ежегодного Доклада по кибербезопасности и за консультирование федерального правительства по всем вопросам, касающимся кибербезопасности. Руководящая группа включает офицеров по связям, работающих с Советом национальной безопасности и экспертов по кибербезопасности из министерств, представленных в Совете национальной безопасности. Директор по информационным технологиям Федеративной Республики Австрия (национальный информационный менеджер) также является членом этого органа. В случае конкретных проблем, если требуется, в Руководящую группу могут входить представители других министерств и австрийских федеральных провинций. Это касается, в частности, ведомств, работающих с организациями и предприятиями, на которые направлены меры, или для которых меры имеют последствия. Представители других, имеющих отношение предприятий, включаются в конкретных случаях, если это необходимо.

2) Создание координационной структуры на оперативном уровне

Оперативная координационная структура будет создана на основе существующих оперативных структур с целью служить платформой для подготовки связанных с конкретными инцидентами и периодических докладов по кибербезопасности и для выработки мер, предпринимаемых на оперативном уровне. Таким образом, она будет обеспечивать постоянно обновляемый обзор развития дел в киберсфере путем сбора, накопления, оценки и передачи адекватной информации. Экономический сектор должен быть подключен соответствующим образом на равноправной основе. Совместный и постоянно обновляемый обзор будет обрисовывать текущее положение в киберсфере и будет служить основой для планирования превентивных и ответных мер. Операторам критической инфраструктуры будет оказываться поддержка на оперативном уровне, и в особенности, в случаях срыва работы информационных и коммуникационных структур. Кроме того, им будет предоставляться информация об угрозах Интернету. Оперативная координационная структура должна быть сформирована таким образом, чтобы ее можно было использовать как оперативный исполнительный орган для помощи руководителям, занимающимся кризисным кибер менеджментом.

Оперативная координационная структура обеспечивает участие министерств, оперативных структур бизнеса и исследовательского сектора. Задачи, выполняемые в Оперативной координационной структуре, координируются Федеральным министерством внутренних дел (в публично-частном партнерстве, или ПЧП). В выполнении координационных функций Федеральному министерству внутренних дел (BMI) поддержку оказывает Федеральное министерство обороны (BMLV), на которое перекладываются функции координации в случае инцидентов в сфере кибероборонны. Все оперативные, организационные, секторные или специфические для определенной целевой группы структуры остаются в компетенции соответствующей организации. Институции, несущие ответственность за вопросы безопасности компьютерных систем, Интернета и защиты критической инфраструктуры, должны взаимодействовать в рамках Оперативной координационной структуры. На национальном уровне, в число таких организаций входят GovCERT (Правительственная группа реагирования на компьютерные инциденты), MilCERT (Военная группа готовности на случай компьютерных инцидентов) и Центр компетентностей по борьбе с киберпреступностью (C4). Другие государственные институции подключаются путем формирования второго круга. Дополнительный круг охватывает частные CERT (CERT.at, BRZ-CERT, банки, и т.д.), а также секторы экономики и исследовательские институты.

Руководящая группа по кибербезопасности формирует *рабочие группы*, отвечающие за подготовку предложений по необходимым процессам и структурам для постоянной координации на оперативном уровне. Соответственно подключаются представители заинтересованных предприятий.

3) Создание системы кибер кризисного менеджмента

Система *Кризисного менеджмента в киберсфере* Австрии включает представителей государства и операторов критической инфраструктуры. В смысле состава и рабочих процессов система определена в Национальной системе менеджмента кризисов и защиты гражданского населения (австрийское сокращение: SKKM). Поскольку охват системы выходит за рамки информационных и коммуникационных технологий (ИКТ), и чтобы обеспечить внутреннюю безопасность в случае всеобъемлющих угроз, Федеральное министерство внутренних дел будет отвечать за координацию кризисного менеджмента. Что касается внешней безопасности, ведущую роль в координации мер по защите суверенитета будет играть Федеральное министерство обороны, обеспечивая национальную оборону (в том числе и кибероборону). Регулярно будут составляться и обновляться *планы по кризисному менеджменту и по осуществлению преемственности* в сотрудничестве с общественными институциями и операторами критической инфраструктуры, основанными на анализе рисков для секторных и межсекторных киберугроз.

Кроме того, *на регулярной основе будут проводится киберучения* для проверки австрийской Системы кризисного менеджмента в киберсфере, а также составляться планы на случай кризисов и для осуществления преемственности.

4) Укрепление существующих киберструктур

Роль GovCERT, подчиняющаяся аппарату федерального канцлера, в качестве государственной ККРЧС, будет расширена. Для этой цели необходимо будет подробно расписать ее правомочия, ответственности и сферы действия, ее институциональное место в рамках публичной администрации, роль в случае кризисов и варианты взаимодействия с Оперативной координационной структурой. Далее следует определить новые требования.

Чтобы избегать и предотвращать киберпреступления, а также для облегчения оперативного международного сотрудничества, следует расширить функции Центра компетентностей по борьбе с киберпреступностью (С4) Федерального министерства внутренних дел. Этот центр является центральным органом Австрии, несущим ответственность за осуществление обязанностей по безопасности и обязанностей уголовной полиции в сфере кибербезопасности.

MilCERT, подчиняющаяся Федеральному министерству обороны, будет расширена для обеспечения оперативных способностей по предотвращению кибератак, для защиты своих собственных сетей и для дальнейшего развития Обзора кибербезопасности. Эти способности, среди прочего, дают возможность создать потенциал для обеспечения ИКТ содействия другим государственным ведомствам.

Будет расширена австрийская *ККРЧС ассоциация* и *CERT.at* для облегчения национального сотрудничества между австрийскими *ККРЧС.* С одной

стороны, это поможет созданию ККРЧС во всех секторах и, с другой, расширит обмен информацией и опытом по вопросам ККРЧС.

Сфера деятельности 2 – Руководство

Цель: В отношение руководства цель состоит в определении роли, ответственностей и полномочия государственных и не-государственных акторов в киберпространстве и создать подходящие условия для сотрудничества между всеми игроками.

Меры:

5) Создание современной регулятивной рамки

При поддержке *Руководящей группы по кибербезопасности* будет подготовлен и внесен в Федеральное правительство комплексный доклад, анализирующий потребность в выработке дополнительных *правовых принципов, регуляторных мер и добровольных обязательств* (кодекс поведения) для гарантирования кибербезопасности в Австрии. Этот доклад будет рассматривать следующие вопросы: создание необходимых организационных структур, распределение задач и полномочий властей, информационный обмен между властями и частными субъектами, обязанность информировать, обязанность принимать защитные меры, а также обеспечение безопасности линий снабжения.

При определении обязанностей не-государственных акторов будет осуществляться баланс между стимулами и санкциями.

6) Определение минимальных стандартов

Все имеющие отношение субъекты должны сотрудничать и определить *минимальные стандарты безопасности* с тем, чтобы обеспечить эффективную превенцию и достижения общего понимания текущих требований. Эти требования должны применяться ко всем компонентам и услугам, используемым во всех связанных с безопасностью ИКТ областях. Применимые нормы, стандарты, правила поведения и передовой опыт будут обобщаться в австрийском *Руководстве по менеджменту информационной безопасности*, которое регулярно будет обновляться.

7) Подготовка ежегодного доклада о кибербезопасности

Руководящая группа по кибербезопасности будет составлять ежегодный доклад, озаглавленный «Кибербезопасность в Австрии».

Сфера деятельности 3 – Сотрудничество между государством, экономикой и обществом

Цель: Многие задачи и ответственности органов публичной администрации, экономических субъектов и мира в целом основаны на информацион-

ных и коммуникационных технологиях (ИКТ). Ответственность за использование цифровых технологий здравомыслящим образом лежит на каждой организационной единице. Однако, только широкое сотрудничество между всеми секторами и постоянный обмен информацией будут способствовать прозрачному и безопасному использованию ИКТ. Поэтому путем осуществления сотрудничества должны усовершенствоваться существующие киберспособности и процессы в администрации, экономике и среди населения, и должны создаваться новые возможности.

Меры:

8) Создание платформы кибербезопасности

Австрийская платформа по кибербезопасности будет функционировать как публично-частное партнерство с целью способствовать коммуникации со всеми заинтересованными лицами из сферы администрации, экономики и академических кругов. Параллельно, существующие инициативы (осуществляемые Австрийским трастовым кругом, организацией Кибербезопасность Австрии, Австрийской независимой некоммерческой ассоциацией по кибербезопасности *Kuratorium Sicheres Österreich* (KSÖ), Австрийским центром по безопасным информационным технологиям (A-SIT) и т.д.) будут и дальше работать и использоваться. Австрийская платформа кибербезопасности будет служить институциональной рамкой для продолжающегося обмена информацией в среде публичной администрации и между администрацией и представителями бизнеса, академических кругов и исследовательских институтов. Все будут участвовать на равных правах в Платформу кибербезопасности, консультируя и поддерживая Руководящую группу по кибербезопасности.

Сотрудничество с частными операторами критической инфраструктуры и с другими экономическими секторами является очень важным для кибербезопасности Австрии. Подробности этого сотрудничества будут обсуждаться в ходе дальнейших разговоров между Руководящей группой по кибербезопасности и экономическим сектором.

Платформа по кибербезопасности будет использоваться для стимулирования обширного *сотрудничества между участвующими партнерами* по таким вопросам, как повышение информированности и подготовки, а также по вопросам исследований и разработок.

Для того, чтобы содействовать достижению общего понимания вызовов и возможностей для действий среди всех партнеров, затронутых проблемами кибербезопасности, необходимо интенсифицировать обмен экспертами между участвующими государственными, частными и научными организациями. При ведущей роли Руководящей группы по кибербезопасности и при поддержке австрийской Платформы по кибербезопасности для этой цели будет разработана специальная программа.

9) Усиление поддержки малых и средних предприятий (МСП)

Для повышения информированности МСП и подготовки их к действиям в опасных ситуациях будет начато выполнение программ по кибербезопасности. Будет поощряться предоставление группами по интересам отобранной онлайн информации для МСП на новом интернет портале, ИКТ безопасность, инициирование кампаний по кибербезопасности для МСП. При поддержке государственных органов, такие специфические для конкретных секторов платформы как Австрийские трастовые круги, будут разрабатывать конкретные для данных секторов планы по оценке рисков. В этот диалог будут включены регуляторные власти и представители заинтересованных субъектов. Эти планы по оценке рисков будут согласованы с государственными планами по кризисному менеджменту и осуществлению непрерывности. Периодически будут организовываться и проводиться межсекторные учения для МСП. По заявкам секторам, в которых работают МСП, будет разрешено участвовать в межсекторных государственных киберучениях.

10) Подготовка Стратегии коммуникации по проблемам кибербезопасности

Чтобы оптимизировать коммуникацию между заинтересованными субъектами из сферы администрации, экономики, академических кругов и общества, все существующие и запланированные к разработке вебсайты должны быть гармонизированы в качестве частей *Стратегии коммуникации по проблемам кибербезопасности*. Эта стратегия коммуникации будет подготовлена Руководящей группой по кибербезопасности и будет включать предложения всех заинтересованных субъектов.

Сфера деятельности 4 – Защита критической инфраструктуры

Цель: Почти все виды инфраструктуры во все большей степени зависят от специализированных ИКТ систем, которые обеспечивают плавное, надежное и непрерывное функционирование в самой большой по возможности степени. Поэтому, первейшей задачей является создание и усовершенствование устойчивых к угрозам информационных систем. В соответствии с Австрийской программой защиты критической инфраструктуры (АПЗКИ) предприятия, эксплуатирующие критическую инфраструктуру, должны применять комплексные архитектуры безопасности. АСКБ направлена на дополнение и усиление этих мер в сфере кибербезопасности. В этом процессе сотрудничество между операторами критической информационной инфраструктуры имеет важнейшее значение.

Меры:

11) Повышение устойчивости критической инфраструктуры

Операторы критической инфраструктуры должны участвовать во всех процессах национального кибер кризисного менеджмента. Таким стратегическим предприятиям ставится задача определить комплексную архитектуру безопасности (менеджмент риска и кризисный менеджмент), обновлять ее

в соответствии с современными угрозами, иметь должность руководящего сотрудника по безопасности и быть готовыми для *кризисной коммуникации*. Также, для этих предприятий должны быть установлены *стандарты по кибербезопасности*, которые должны применяться в духе партнерства.

Операторы критической инфраструктуры обязаны докладывать о *тяжелых кибер инцидентах*. После комплексных консультаций с касающимися заинтересованными субъектами должна быть создана соответствующая юридическая основа для этого.

Существующие положения *Программы защиты критической инфраструктуры* (АПЗКИ) должны оцениваться на регулярной основе для гарантирования непрерывного противодействия новым киберугрозам и изменяться, если это необходимо.

Сфера деятельности 5 – повышение информированности и подготовки

Цель: Все целевые группы должны быть ознакомлены с проблемами кибербезопасности для того, чтобы повысить свою информированность, заинтересованность и уделяемое этим проблемам внимание. Меры по повышению информированности будут способствовать формированию понимания необходимости обеспечения кибербезопасности. Конкретные для целевой группы меры должны передавать и пропагандировать необходимые знания о кибербезопасном поведении, ответственном использовании информации и ИКТ инструментов в целом. Повышенная подготовка по вопросам кибербезопасности в школах и других образовательных заведениях, а также добавление компетентности по кибербезопасности к преподаванию, должны обеспечивать значимый и адекватный уровень ИКТ компетентности.

Меры:

12) Повышение культуры кибербезопасности

Разрабатываются, координируются и осуществляются инициативы по повышению осведомленности в согласие с общим подходом, реализованным в существующих программах. При этом важно рассматривать кибербезопасность с разных точек зрения, подчеркивая соответствующие опасности, привлекая внимание к возможным последствиям и потерям, а также давать рекомендации по мерам безопасности.

Для того, чтобы дать разным целевым группам доступ к более углубленным конкретным советам, следует далее развивать и расширять существующие *программы по консультированию*.

Будет создан веб-базированный *Интернет портал по ИКТ безопасности*, который будет служить информационным и коммуникационным центром для повышения осведомленности. За координацию работы Интернет

портала по ИКТ безопасности будут отвечать Министерство финансов, администрация канцлера и A-SIT. Стратегический подход этого портала должен руководствоваться принципами и целями АСКБ.

Будут разрабатываться и развиваться *превентивные программы* по защите от киберпреступлений.

13) Интегрирование кибербезопасности и медиа грамотности на всех уровнях образования и квалификации

Австрия будет стремиться к более существенной интеграции грамотности по ИКТ, по кибербезопасности и медиа грамотности в *школьные программы*. Грамотность по ИКТ и медиа грамотность являются частью программ всех видов школ. Проблемы ИКТ безопасности и кибербезопасности в итоге станут интегральной частью модели, названной *Цифровая компетентность*. Эта модель будет приспособлена к программам соответствующего вида школ, будет обеспечивать осведомленность о проблемах безопасности и будет способствовать безопасному и ответственному использованию Интернета. Цель состоит в том, чтобы обеспечить определенный уровень ИКТ компетентности во всех видах школ.

Компетентность по ИКТ (безопасности) должна быть частью *академической подготовки* в педагогических университетах, а также в педагогических институтах высшего образования. Учителям будет нужно получить кибер образование перед тем, как они начнут преподавать кибер умения в средних школах или в образовательных центрах для взрослых.

Подготовка *экспертов в публичном секторе*, ответственных за повышение кибербезопасности, будет интенсифицирована в сотрудничестве с международными и национальными институтами квалификации.

Администраторы ИКТ систем, работающие на операторов критической инфраструктуры, должны получить дополнительную подготовку по кибербезопасности для того, чтобы они могли распознавать кибер инциденты, выявлять аномалии в их ИКТ системах и докладывать о них администраторам по безопасности (*Программа регистрации инцидентов с использованием человека в качестве датчика)*.

Сфера деятельности 6 – исследования и разработки

Цель: Обеспечить технологическую экспертизу по кибербезопасности, основанную на результатах самых передовых исследований и разработок. Для этого вопросы кибербезопасности должны быть во все большей степени интегрированы в прикладные кибер исследования и в исследовательские программы по безопасности, например, в австрийскую программу KIRAS. Необходимо вкладывать ресурсы для достижения лидерства по этой теме в исследовательских программах ЕС по безопасности.

Меры:

14) Интенсификация австрийских исследований по кибербезопасности

В охвате национальных программ и программ ЕС исследований по безопасности, *кибербезопасность* должна стать *ключевым приоритетом*. Через совместные проекты соответствующие заинтересованные субъекты из администрации, деловой сферы и исследовательских организаций разработают концептуальную рамку и технологические инструменты для повышения потенциала по кибербезопасности Австрии. Особый упор следует ставить на меры, способствующие быстрому превращению результатов исследований и разработок в коммерческие продукты. Существующие исследовательские проекты, например те, что курируются A-SIT, должны и далее развиваться.

Австрия должна стремиться к активной ведущей роли по определенным темам в исследовательских программах ЕС по безопасности. Для этого Австрия должна инициировать включение кибер тем, которые важны для Австрии, в международные исследовательские программы.

Сфера деятельности 7 – международное сотрудничество

Цель: Глобальная сетевая работа и международное сотрудничество являются ключевыми факторами в АСКБ. Безопасность в киберпространстве можно обеспечить только через координированное сочетание политик на национальном и международном уровнях. Поэтому Австрия будет осуществлять активную внешнюю кибер политику и следовать своим интересам скоординированным и целенаправленным образом в рамках ЕС, ООН, ОБСЕ, Совета Европы, ОЭСР и НАТО. Кроме того, международные аспекты австрийской киберполитики будут соответственно гармонизированы с другими сферами политики.

Меры:

15) Эффективная коллаборация по кибербезопасности в Европе и в мировом масштабе

Австрия будет давать существенный вклад в развитие и реализацию *Стратегии кибербезопасности ЕС.* Она будет в полной мере участвовать в стратегической и оперативной работе ЕС.

Соответствующие министерства будут принимать необходимые меры для реализации и полного использования *Конвенции о киберпреступности* Совета Европы.

На международном уровне Австрия поддерживает свободу Интернета, которая гарантирует свободное упражнение всех *прав человека в виртуальном пространстве*. В частности, свобода выражения и информация не должны ограничиваться в Интернете без правовых оснований. Это позиция, которую Австрия защищает на международных форумах. Поэтому Австрия активно будет участвовать в разработке и установлению транснационального кодекса поведения для деятельности государств в киберпространстве, что также будет включать меры по укреплению доверия и безопасности.

Австрия продолжит двустороннее сотрудничество, инициированное в рамках Партнерства ради мира НАТО, и будет активно поддерживать подготовку списка конкретных мер по укреплению доверия и безопасности в рамках ОБСЕ.

Австрия уже активно принимает участие в планировании и проведении *транснациональных кибер учений*. Опыт, приобретаемый на таких учениях, будет использоваться напрямую при планировании и дальнейшем развитии оперативных программ.

Внешнеполитические меры, касающиеся кибербезопасности, координируются Федеральным министерством Европы, интеграции и иностранных дел (ФМЕИИД). Когда это оправдано, будет рассматриваться заключение двухсторонних или международных соглашений.

Структуры, осуществляющие политику в общенациональном контексте

В Австрии менеджмент кибер проблем координируют следующие структуры. На высшем уровне, т.е. *политическом*, политические и стратегические цели определяет австрийское правительство. *Совет национальной безопасности (СНБ)* функционирует в качестве консультативного органа по национальной безопасности на *стратегическом уровне*. В случае кибер инцидента, СНБ привлекает *Руководящую группу по кибербезопасности (РГКБ)*. РГКБ координирует меры по кибербезопасности на политико-стратегическом уровне под руководством администрации федерального канцлера. Он осуществляет мониторинг и поддерживает реализацию АСКБ, составляет ежегодный доклад по кибербезопасности и консультирует федеральное правительство по вопросам кибербезопасности.

В случае кибер инцидентов поддержку обеспечивает и *Платформа по кибербезопасности (ПКБ*). ПКБ является основной платформой для осуществления сотрудничества и обмена информацией между субъектами бизнеса, науки, исследований, критической инфраструктуры и публичной администрации.

В зависимости от типа киберугрозы на оперативном уровне задачи возлагаются или на *Внутренний круг оперативной координации* (ВКОК), или на *Расширенный круг оперативной координации* (РКОК).

ВКОК отвечает за оперативное управление и координацию в кибер сфере. Он поддерживает контакт с операторами критической инфраструктуры, бизнесом и отделами министерств, работающими в кибер сфере, разрабатывает стандарты и оперативные меры, применяемые в случае кибер инцидентов. ВКОК также служит интеграционной платформой для обмена информацией. Он разрабатывает промежуточный, связанный с инцидентами обзор кибербезопасности и обсуждает необходимые оперативные меры. Он предоставляет постоянно обновляемый обзор ситуации в кибер сфере путем сбора, компилирования, оценки и передачи соответствующей

информации. ВКОК состоит из представителей администрации федерального канцлера, министерства внутренних дел (МВД), МО и ФМЕИИД, Центр кибербезопасности (ЦКБ; МО) и Центр кибер обороны (ЦКО; МО), которые председательствуют ВКОК, и включает также и другие государственные акторы/ведомства. Это означает, что все кибер активы национального кибер сообщества включены в ВКОК: ЦКБ и С4 МВД; ЦКО и MilCert МО; GovCERT; и т.д.

Фигура 1: Постоянная структура для оперативной координации.

Что касается *GovCert*, то она является сверхструктурой всех государственных ККРЧС и играет ведущую роль в публичной администрации.

РКОК по существу является расширенным ВКОК плюс Ассоциация CERT. Ассоциация *CERT* усиливает ККРЧС структуры на национальном уровне. Она интенсифицирует совместные усилия специфическими для конкретных секторов ККРЧС (участвуя в определенных секторах критической инфраструктуры).

На национальном уровне имеются и гражданские агентства с подобными функциями, работающие наряду с государственными ККРЧС. Они предназначены, прежде всего, для кризисных интервенций в случае кибератак против гражданских компаний или делового сектора. Эти гражданские агентства организованы в группы по секторам. CERT.at является их

сверхструктурой и, в сотрудничестве с Администрацией канцлера, создала Австрийский трастовый круг. Австрийский трастовый круг предоставляет формальную рамку для обмена информацией по безопасности между CERT.at, Администрацией канцлерства и GovCERT. В рамках этого партнерства предвидится связать все австрийские ККРЧС для обсуждения стандартов, оказания помощи пострадавшим компаниям и деловым секторам и разработки совместных стратегий на случай кибератак.

Основные ответственности

МВД отвечает за борьбу с *киберпреступностью* и за *защиту критической инфраструктуры*.

МО на первом месте отвечает за кибер *оборону* и за ее три составляющих: *киберразведку* (осуществляемую Службой охраны вооруженных сил и Службой разведки вооруженных си), *ИКТ безопасность* (сфера деятельности Центра ИКТ и кибер безопасности) и *кибер операции* (сфера действия Командования вооруженных сил). Кроме того, в случае кибер инцидентов вооруженные силы содействуют для обеспечения поддержки всей миссии.

ФМЕИИД отвечает за *кибер дипломатию*.

Ответственности в случае кибер инцидентов

В Австрии имеются *три уровня киберугроз*, определяемые степенью эскалации кибер риска.

Первый уровень относится к *стандартным кибер операциям*, при которых следует осуществлять менеджмент соответственно в случаях кибер преступлений, кибер шпионажа и кражи данных. На этом уровне за координацию реакции отвечает МВД. МВД координирует тесное сотрудничество, обмен информацией и взаимную поддержку между всеми заинтересованными субъектами, используя возможности ВКОК. МО должно быть в состоянии предпринимать соответствующие действия в рамках своей ответственности и, если это необходимо, оказывать поддержку публичным институциям при просьбе о содействии.

Второй уровень касается *кибер кризисов*, когда адекватно надо справляться с инцидентами в диапазоне от кибератак на критическую инфраструктуру до выключений света в результате кибератак. На этом уровне за координацию реакции тоже несет ответственность МВД. МВД координирует тесное сотрудничество, обмен информацией и, если необходимо, взаимную поддержку между всеми заинтересованными субъектами. На стратегическом уровне активируется Руководящая группа по кибербезопасности, и она берет на себя руководство ВКОК и ЦКБ МВД. И снова, МО должно быть в состоянии предпринимать соответствующие действия в охвате своей ответственности и, если это необходимо, оказывать поддержку другим ведомствам при просьбе о содействии.

Третий уровень касается *кибер обороны*, когда политически мотивированные атаки составляют существенную угрозу для суверенитета государ-

ства. В этом случае, координация реакции возлагается на МО. На стратегическом уровне активируется Руководящая группа по кибербезопасности, и она берет на себя руководство ВКОК и ЦКО МО для действий на оперативном уровне. МО координирует осуществление тесного сотрудничества, обмен информацией и, если это необходимо, взаимную поддержку между заинтересованными субъектами.

Надо отметить, что систематический трансфер ответственности от МВД к МО не может быть осуществлен категорически или распланирован в деталях в случае кибер кризиса, переходящего в кибер оборону. Был разработан контрольный список условий для такого трансфера. В случае реального кибер инцидента, однако, трансфер правомочий следует определять на основе тщательной оценки ситуации.

Реализация политики кибербезопасности в МО и Вооруженных силах Австрии

АСКБ 2013 возложила на Федеральное министерство обороны (ФМО) выполнение важных задач и мер. Также Министерству обороны (МО) вменяются обязанности Стратегией обороны от 2014 (СО14) и Военной стратегией от 2017 (ВС17). До сих пор МО работало с существующими концептуальными документами. В данное время, МО разрабатывает Стратегию кибер обороны (СКО) и Концепцию военных кибер операций (ВКО).

Структурная реформа национальной обороны от 2016 года (LV21.1) создала «Командование Коммуникационных и информационных систем и кибер обороны» (Командование КИС & КО; KdoFüU&CD), которое является отдельным видом вооруженных сил, осуществляющем оперативное руководство и располагающее кибер способностями. Таким образом, почти все способности в сфере поддержки командования, ИКТ, электронной борьбы, кибер обороны и навигационных операций были сведены в единое командование.

По бюджетным причинам, от этой амбициозной цели отказались, и в 2109 Командование КИС и КО было расформировано. В настоящее время ответственность за кибер оборону несут следующие военные структуры:

- Объединенное командование сил (ОКС), которое отвечает за кибер операции (КиОп).
- Центр КИС и кибербезопасности (ЦКИСКБ), который несет ответственность за ИКТ оборону.
- Две военные разведывательные службы – Управление безопасности вооруженных сил (УБВС) и Австрийское управление стратегической разведки (УСРА) — они отвечают за сферу кибер разведки (КиРаз).

Австрийская военная кибер оборона сосредоточена на защите сети и будет расширяться в соответствие со среднесрочными и долгосрочными целями развития вооруженных сил.

Ключевые национальные инициативы и вызовы политике реагирования Австрии

В настоящее время, основным вызовом является полная реализация на национальном уровне политики, основанной на общем для ЕС законодательстве по кибербезопасности, известном как Директива о сетевой и информационной безопасности (Директива СИБ). Эта директива задает курс для повышения безопасности сетей и информационных систем в долгосрочном плане. Прежде всего, будет повышена безопасность конкретной критической инфраструктуры в разных секторах.

Кроме этого, как выше уже было сказано, на национальном уровне разрабатывается общегосударственная Австрийская стратегия кибербезопасности.

Далее, совместная работа на всех уровнях интенсифицируется. С одной стороны, укрепляется сотрудничество на национальном уровне между публичными субъектами и субъектами частного бизнеса, а также кооперация между вооруженными силами и гражданским сектором. С другой стороны, расширяются совместные усилия между Австрией и международными организациями, ЕС и НАТО. Что касается ЕС, в кибер сфере инициируются проекты в рамках Постоянного структурированного сотрудничества (PESCO).

Австрийские вооруженные силы (Österreichisches Bundesheer) также используют преимущества, которые дают знания, предоставляемые Центром передового опыта НАТО по совместной кибер обороне (CCDCOE), являющегося многонациональным и интердисциплинарным центром по кибер обороне.

Также австрийские вооруженные силы принимают участие в совместных международных учениях, предназначенных для развития киберспособностей и оперативной совместимости в кибер обороне. Австрия, Германия и Швейцария принадлежат к странам трехстороннего сотрудничества «D-A-CH» и *ежегодно* проводят учения по оперативной совместимости. Австрия регулярно принимает участие в этих учениях и также приняла участие в учении по оперативной совместимости *Общая крыша* 2018.

Австрия регулярно участвует в таких больших учениях, как *Сомкнутые щиты*, международное техническое реальное учение по кибер обороне, организуемое центра CCDCOE НАТО, или технологично-ориентированное *KSÖ-Planspiele*, симулятивное учение по кибербезопасности, организуемое на национальном уровне Kuratorium Sicheres Österreich (KSÖ), австрийской независимой некоммерческой ассоциацией, стремящейся к повышению безопасности Австрии, учение *Коалиционный воин* по исследованию, экспериментированию, испытанию и упражнению оперативной совместимости (CWIX), мероприятие НАТО по оперативной совместимости Cyber.PHALANX

2018, учение для военных планировщиков и штабов, и Австрийское учение по принятию стратегических решений ASDEM18, и это только некоторые из числа хорошо известных учений.

Стоит упомянуть, что Австрия является стороной во множестве двухсторонних отношений сотрудничества, на первом месте с другими государствами-членами Европейского Союза, но также и с Вооруженными силами Израиля.

Кроме того, каждый год Австрия проводит мероприятие *Вызов по кибербезопасности Австрия*, которое является состязанием для национального поиска талантов. Команды-победители представляют Австрию на соревновании *Вызов по кибербезопасности Европа*.

Привлечение австрийского частного сектора и академических кругов

В частном секторе стоит упомянуть исследовательскую и технологическую деятельность Австрийского института технологии (АИТ) и работу организации KSÖ. В академическом секторе упоминания заслуживают Университет технологии Граца и Кампус кибербезопасность Граца (партнерство между Университетом технологии Граца и SGS), Кампус Хагенберг Университета прикладных наук Верхней Австрии и Университет прикладных наук Санкт-Пельтен.

Перед исключительными ограничениями

В австрийском контексте следует иметь ввиду следующие ограничения:

- Бюджетное давление на оборонные расходы, которые на сегодняшний день составляют 0.58% ВВП.
- Правовая рамка, которая на данный момент позволяет проведение наступательных кибер операций только в случае инцидентов, категорированных как «национальная кибер оборона». Согласно текущему законодательству, кибератаки ниже уровня угроза для кибероброны (на уровне «стандартные кибер операции» или «кибер кризис») не разрешены.
- Фундаментальной проблемой стало рекрутирование кибер экспертов. В настоящее время образовательная инфраструктура Австрии не производит требуемое количество специалистов для покрытия потребностей публичного сектора, вооруженных сил и частного бизнес сектора. В результате, налицо яростная конкуренция для привлечения лучших экспертов. Тем не менее, благодаря призывной системе, у австрийских вооруженных сил имеется определенное преимущество перед другими публичными ведомствами и экономикой, поскольку вооруженные силы располагают квалифицированными кибер и ИКТ специалистами на регулярной или временной основе. Эти кибер рекруты получают дополнительную квалифика-

цию во время своей военной службы и их опыт используется эффективно. Также, кибер специалистов, которые призываются как кибер эксперты для военных целей, включает система австрийской милиции.

В качестве следующего шага кибер образования Австрия рассматривает создание отдельной военной системы квалификации в кибер сфере и ИКТ. Предпринимаются шаги к организации кибер квалификации, позволяющей специальные карьерные пути развития для сержантского и офицерского состава. Это будет гарантировать, что вооруженные силы смогут использовать свой собственный личный состав с кибер и ИКТ квалификацией.

- Недостатком для кибер обороны является то, что кибер эксперты Австрийских вооруженных сил не являются частью сообщества Платформы для обмена информации о вредоносных программах Агентства коммуникации и информации НАТО.

Путь вперед

Из-за существенного развития состояния военных кибер дел было бы полезно пойти даже дальше, чем текущие, уже весьма амбициозные работы ЕС (к примеру, под руководством Агентство ЕС по кибербезопасности ENISA (бывшее Агентство сетевой и информационной безопасности Европейского Союза), команды реагирования на компьютерные чрезвычайные ситуации разных институций ЕС, и т.д.) и создать центральный кибер офис или кибер ячейку в Военном штабе Европейского Союза. Было бы более полезно, чтобы государства-члены ЕС могли бы управлять делами как сверху вниз, так и снизу-вверх.

Текущая программа австрийского правительства предвидит создание Национального центра кибербезопасности для Австрии, включающего всех главных государственных игроков. Такой центр будет очень важным и, после учреждения и приведения в оперативную готовность, он существенно улучшит эффективность, поток информации, анализ ситуационной осведомленности и скорость реагирования.

Определенно, было бы полезно, если бы NATO CCDCOE расширил портфолио своих задач и создал центр для всех уровней кибер дел (стратегический, оперативный, тактико/технический, исследовательский).

Кроме того, рекомендуется, чтобы Европа под руководством ЕС начала выполнять существенные кибер усовершенствования, в том числе такие кибер меры, как развитие *кластеров кибер технологий* (например, определяя какие страны присоединяются или берут на себя руководство в каких областях исследований или кибер индустрии), повышение технической безопасности сетей и создание европейских *стандартов* для разных инженерных решений с целью достижения более высокой степени безопасности путем встраивания искусственного интеллекта в будущие ИКТ, оружейные и сенсорные системы с самого начала проектирования.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами авторов и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Признательность

Том 19 журнала *Connections: The Quarterly Journal* публикуется при поддержке правительства Соединенных Штатов Америки.

Об авторе

Бригадный генерал **Герман КАПОНИГ** является киберкоординатором австрийского Министерства обороны. До этого он служил начальником Командного центра поддержки Вооруженных сил Австрии, начальником логистической дирекции МО и начальником Отдела планирования и вооружений в кабинете федерального министра обороны и спорта.