ОБОСНОВАНИЕ ПОТРЕБНОСТИ В МЕТОДИКЕ ОЦЕНКИ КАЧЕСТВА И ЭФФЕКТИВНОСТИ КОМПЛЕКСНОЙ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В МЧС РОССИИ

А.Ю. Ярошенко.
Национальный центр управления в кризисных ситуациях МЧС России.
М.В. Буйневич, доктор технических наук, профессор.
Санкт-Петербургский университет ГПС МЧС России

Рассматривается негативное влияние несистемного применения средств защиты информации в условиях доминанты «документационного» обеспечения информационной безопасности на состояние защищенности информационно-телекоммуникационной структуры МЧС России. Показывается, как количество и разнообразие одновременно используемых компонент защиты приводит к необходимости создания комплексных организационно-технических систем обеспечения безопасности информации. Делается вывод, что отсутствие возможности оценки качества построения и эффективности функционирования таких систем диктует потребность в научной разработке соответствующей методики.

Ключевые слова: угрозы информационной безопасности, средства защиты информации, комплексная организационно-техническая система обеспечения безопасности информации, эффективность и качество построения и функционирования, методика оценки

THE REASONS FOR NECESSITY IN TECHNIQUE OF QUALITY ASSESSING AND EFFICIENCY OF COMPLEX ORGANIZATIONAL AND TECHNICAL INFORMATION SECURITY SYSTEM IN EMERCOM OF RUSSIA

A.Yu. Yaroshenko. National crisis management centre of EMERCOM of Russia.
M.V. Buinevich. Saint-Petersburg university of State fire service of EMERCOM of Russia

The article describes the negative impact of non-systemic use of information security means in the conditions of dominant «documentation» support of information security on the security state of information and telecommunication structure of EMERCOM of Russia. It is shown how the number and variety of simultaneously used protection components lead to the creation necessity of complex organizational and technical information security systems. There is the conclusion that the inability to evaluate the construction quality and operation efficiency of these systems dictates the necessity for development of an appropriate technique.

Keywords: information security threats, information security means, complex organizational and technical information security system, efficiency and quality of construction and operation, evaluation technique

Повсеместное использование в МЧС России информационных технологий значительно увеличивает количество угроз информационной безопасности (ИБ), следствием реализации которых может стать утечка конфиденциальных данных, нарушение целостности и доступности критической информации, например, персональных данных ответственных сотрудников МЧС России и других граждан Российской Федерации в рамках исполнения

МЧС России своих задач и функций, а также иных сведений, которые содержатся в государственных информационных системах МЧС России [1–3].

Разнообразие средств информационных технологий и порождаемых ими угроз не позволяет создать универсальный механизм обеспечения ИБ, что с неизбежностью ведет к лавинообразному росту количества применяемых средств защиты информации (СрЗИ), привлекаемых человеческих, временных, финансовых и прочих ресурсов, используемых нормативных правовых актов и руководящих документов, регламентирующих их взаимоотношения и взаимодействие. Рассмотрим эти компоненты защиты информации более подробно.

В компьютерных сетях МЧС России внедрены и функционируют различные СрЗИ, в том числе межсетевые экраны, антивирусные программы, системы обнаружения вторжений и др. Но значительная часть этих средств имеет настройки «по умолчанию», без привязки к тем информационным и телекоммуникационным системам, в среде которых они функционируют и ИБ которых они призваны обеспечить.

Например, межсетевой экран, основной функцией которого является фильтрование трафика, без дополнительных настроек выполняет лишь функции маршрутизатора, пропуская через себя весь, в том числе нелегитимный трафик. Наличие на внутреннем сетевом интерфейсе в конце списка правил фильтрации строки «Permit ip any any», по сути, нейтрализует все запрещающие правила, находящиеся выше по списку, открывая безграничный сетевой доступ пользователям локальной сети. Наличие такого правила на внешнем интерфейсе обеспечивает не только злоумышленникам, но и случайным пользователям, находящимся за пределами организации, полный доступ к ресурсам организации [4].

Средства криптографической защиты информации (СрКЗИ), призванные обеспечить конфиденциальность и целостность передаваемой по выделенным или арендованным каналам связи между различными подразделениями МЧС России информации, могут, как и межсетевые экраны, быть настроенными как обычный маршрутизатор либо отсутствовать вовсе, ввиду отсутствия финансирования. Кроме того, зачастую СрКЗИ физически размещают в стороне от основного канала передачи данных, логически перенаправляя на СрКЗИ трафик, подлежащий шифрованию. Следствием возможных сбоев в сети передачи данных будет абсолютное исключение СрКЗИ из логической схемы шифрования. В каждом из перечисленных случаев попадает под сомнение выполнение требований законодательства и регуляторов в области криптографической защиты конфиденциальной информации.

Система обнаружения вторжений без выполненных должным образом настроек собирает большое количество ложноположительных (false positive), ложноотрицательных (false negative), истинно положительных (true positive) и истинно отрицательных (true negative) уведомлений об инцидентах ИБ, дифференцирование которых для неподготовленных администраторов безопасности может стать непосильной задачей. Объем собранной информации затрудняет ее анализ и своевременное обнаружение вторжений, в результате чего система обнаружения вторжений работает как «черный ящик», не оказывая никакого влияния на состояние ИБ.

Зачастую (вследствие отсутствия необходимого обучения сотрудников, отвечающих за ИБ) СрЗИ от несанкционированного доступа устанавливаются с настройками по умолчанию, поэтому часть необходимых функций остается неиспользованной. Администратор безопасности может и не подозревать о наличии в этих СрЗИ по умолчанию отключенных, но способных закрыть тот или иной пробел в выполнении функций, требуемых согласно нормативно-правовым актам и руководящим документам. Наряду с другими, одной из таких функций является принудительное задание сложности пароля пользователя Active Directory вне зависимости от сложности пароля, заданной в политике безопасности доменной структуры.

Также антивирус, установленный «как есть», может не выполнять основные защитные функции или, напротив, может удалять легитимные файлы и программы, даже если они

выполняют заявленные функции, но были написаны много лет назад и не обновлялись. В последнем случае пользователь зачастую отключает антивирусную программу, которая «мешает» работать, тем самым повышает угрозу ИБ не только для своего рабочего места, но и для информационной системы в целом.

Таким образом, применение для решения задач ИБ разнообразных СрЗИ носит взаимообусловленный и взаимопротиворечивый характер: применение рекомендованных и призванных минимизировать риски ИБ настроек на одних средствах может нести негативные последствия при использовании других.

Все вышеперечисленные ситуации и многие другие, не рассмотренные здесь, могут быть следствием отсутствия в организациях МЧС России необходимого количества компетентных специалистов в области ИБ и некорректного разделения функциональных обязанностей в организационно-штатной структуре организации.

Обязанности администраторов безопасности нередко возлагаются на сотрудников организации, не имеющих должного уровня знаний и соответствующего профильного образования или на должностных лиц, служебные обязанности которых связаны с обеспечением непрерывности работы сетей связи и происходящих в организации информационных процессов. Как следствие – приоритетом для таких сотрудников становится исполнение непосредственных обязанностей, а выполнение требований ИБ носит для них обременительный характер.

Несогласованность действий администраторов систем и администраторов безопасности может также привести к негативным последствиям. Так, например, развернутые без согласования со службой ИБ программное обеспечение или программно-аппаратные комплексы могут сами нести в себе угрозу, если в них содержатся «закладки» или сама компания-интегратор оставляет себе возможность дистанционного подключения к развернутой системе для ее удаленного администрирования (backdoor).

Администраторы систем могут игнорировать требование своевременного обновления общесистемного и специализированного программного обеспечения, используемого во внутренней сети организации, аргументируя это тем, что внутренняя сеть физически отделена от сетей международного обмена «Интернет» либо для сопряжения этих сетей используется сертифицированный межсетевой экран, тем самым открывая дополнительные возможности для проведения целенаправленных атак, эксплуатирующих уязвимости программного обеспечения [5–8].

Такое положение дел негативно влияет на состояние защищенности информационно-телекоммуникационной структуры организации, может стать причиной инцидентов взлома компьютерной сети, блокирования ее работы и т.п.

Большое количество и разнообразие Федеральных законов Российской Федерации, Указов Президента и Постановлений Правительства Российской Федерации, руководящих документов регуляторов в сфере ИБ (таких как федеральная служба безопасности и федеральная служба по техническому и экспертному контролю (ФСТЭК) России), объем которых эквивалентен нескольким томам, и в которых изложены требования к компонентам защиты информации, а также стремительно выпускаемые дополнения и изменения к этим нормативно-правовым актам и распорядительным документам, не позволяют специалистам по ИБ в полной мере осмыслить и реализовать все выдвигаемые требования.

Так, например, согласно опубликованным результатам исследования, проведенного М.В. Буйневичем [9], на официальном сайте только одного регулятора (ФСТЭК России) в разделе «Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы...» и только по вопросам технической защиты информации размещено свыше 30 только «открытых» документов общим объемом 14 304 kB или 1 172 страницы (и это не считая свыше 60 ссылок на стандарты).

Кроме того, согласно требованиям нормативно-правовых актов Российской Федерации в области ИБ (специфицированных регуляторами в соответствующих руководящих документах) в каждой организации должен быть сформирован пакет

внутренних регламентирующих документов, содержащих в себе инструкции по настройке межсетевых экранов, по антивирусной и парольной защите, по обнаружению инцидентов ИБ и реагированию на них и многие др. На состав и содержание этих документов также влияют потребности внутренних бизнес-процессов.

Этот гигантский вал нормативно-правовых актов, руководящих и регламентирующих документов приводит к смещению доминанты обеспечения реальной ИБ в сторону ее «документационного» обеспечения – к, так называемому, обеспечению ИБ «на бумаге».

Гармоничное же (непротиворечивое) существование и совместное функционирование рассмотренных выше компонентов защиты, а именно: программно-аппаратных средств защиты информации, регламентирующих документов и кадрового состава, возможно только в составе некой комплексной организационно-технической системы обеспечения безопасности информации (КОТСОБИ).

Здесь следует отметить принципиальное отличие КОТСОБИ от традиционных систем комплексной защиты информации, которое заключаются в трактовке понятия «комплексный». Если во втором случае обсуждаемый термин применяется для характеристики количества «закрываемых» каналов утечки информации и деструктивного воздействия (технические, физические, программные и т.д.), то в первом он характеризует вышеупомянутую совокупность всех компонент защиты: программно-технической, организационной, правовой, кадровой и т.д.

Для сохранения требуемого качества и высокой эффективности КОТСОБИ в условиях роста угроз ИБ ее необходимо непрерывно развивать и совершенствовать (модернизировать), внедряя современные СрЗИ, поддерживая требуемый штат и уровень компетенции сотрудников, а также необходимый и достаточный состав регламентирующих документов.

Но эта декларация на практике выглядит весьма проблематичной. Так, в больших территориально-распределенных сетях государственных организаций, таких как МЧС России, где количество отдельно расположенных территориальных органов по всей территории Российской Федерации может достигать нескольких тысяч, а поддержание информационно-телекоммуникационной системы в рабочем состоянии играет обеспечивающую роль, централизованное внедрение программных и программно-аппаратных СрЗИ, а также регламентирующих документов, крайне затруднительно из-за финансовых, профессиональных, кадровых, организационных и других проблем. Зачастую решения о внедрении принимаются спонтанно фрагментарно; за основу таких решений берутся «вырванные» из контекста отдельные положения нормативно-правовых актов и руководящих документов регуляторов, выводы после посещения различных конференций (организованных, в том числе, коммерческими структурами), рекомендации многочисленных отечественных и международных стандартов в области ИБ (их аналитический обзор для телекоммуникационных сетей выполнен в работе [10]). Как следствие, развитие КОТСОБИ носит случайно-субъективный (и, соответственно, далеко не оптимальный) характер, внося еще больше неопределенности в существующее состояние дел с защитой информации и планы по ее совершенствованию.

Весть этот «бумажный арсенал» не предлагает соответствующего методического инструмента для оценки качества и эффективности КОТСОБИ. В результате ответственный за защиту информации и курирующее ее руководство организации зачастую остаются в неведении касательно животрепещущих вопросов обеспечения ИБ, а именно: 1) насколько существующая КОТСОБИ соответствует многочисленным требованиям регуляторов? 2) какие действия необходимо предпринять в первую очередь (обучить персонал, закупить СрЗИ, разработать регламентирующие документы и пр.) и на что потратить всегда ограниченные ресурсы? 3) каков бизнес-план развития инфраструктуры КОТСОБИ в краткосрочной, среднесрочной и долгосрочной перспективе? Следует помнить, что цена ошибочных ответов на эти вопросы бывает крайне высокой.

Именно поэтому экспертному и научному сообществу в кооперации со специалистами МЧС России (при патронаже регуляторов) необходимо разработать и повсеместно внедрить

единую и достаточно универсальную методику оценки качества построения и эффективности функционирования КОТСОБИ, которая позволит выявить недостатки в построении системы, определить возможные действия для устранения этих недостатков в ближайшее время и запланировать мероприятия по ее совершенствованию.

Литература

1. Богданов А.В., Примакин А.И., Синещук М.Ю., Синещук Ю.И. Основные угрозы и направления обеспечения безопасности единого информационного пространства // Вестник Санкт-Петербургского университета МВД России. 2013. Т. 58. № 2. С. 150–153.

2. Синещук Ю.И., Власов С.В., Синещук М.Ю. Задачи формирования и основные компоненты единого информационного пространства МЧС России // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2012. № 2. С. 75–79.

3. Примакин А.И., Синещук Ю.И., Пантиховский О.В., Синещук М.Ю. Правовые аспекты безопасности единого информационного пространства силовых ведомств (МВД, МЧС, МО) // Вестник Санкт-Петербургского университета МВД России. 2012. Т. 54. № 2. С. 234–240.

4. Ярошенко А.Ю. Системный подход к настройке и внедрению межсетевых экранов в государственные информационные системы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сборник научных статей. 2016.

5. Буйневич М.В., Израилов К.Е., Мостович Д.И., Ярошенко А.Ю. Проблемные вопросы нейтрализации уязвимостей программного кода телекоммуникационных устройств // Проблемы управления рисками в техносфере. 2016. №. 3(39). С. 81–89.

6. Буйневич, М.В., Щербаков, О.В., Владыко, А.Г., Израилов, К.Е., Архитектурные уязвимости моделей телекоммуникационных сетей // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2015. № 4. С. 86–93.

7. Буйневич М.В., Щербаков О.В., Израилов К.Е. Структурная модель машинного кода, специализированная для поиска уязвимостей в программном обеспечении автоматизированных систем управления // Проблемы управления рисками в техносфере. 2014. № 3 (31). С. 68–74.

8. Буйневич М.В., Израилов К.Е., Щербаков О.В. Модель машинного кода, специализированная для поиска уязвимостей // Вестник Воронежского института ГПС МЧС России. 2014. № 2 (11). С. 46–51.

9. Буйневич М.В., Примакин А.И. Категориальный анализ проблем гармонизации нормативно-правовой базы информационной безопасности // Информационная безопасность регионов России (ИБРР-2015): материалы IX Санкт-Петербургской межрегион. конф., Санкт-Петербург, 28–30 окт. 2015 г. СПб.: СПОИСУ, 2015. С. 34–35.

10. Буйневич М.В., Владыко А.Г., Доценко С.М., Симонина О.А. Организационно-техническое обеспечение устойчивости функционирования и безопасности сети связи общего пользования. СПб.: СПбГУТ, 2013. 144 с.

References

1. Bogdanov A.V., Primakin A.I., Sineshchuk M.Yu., Sineshchuk Yu.I. Osnovnye ugrozy i napravleniya obespecheniya bezopasnosti edinogo informacionnogo prostranstva // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2013. T. 58. № 2. S. 150–153.

2. Sineshchuk Yu.I., Vlasov S.V., Sineshchuk M.Yu. Zadachi formirovaniya i osnovnye komponenty edinogo informacionnogo prostranstva MCHS Rossii // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MCHS Rossii». 2012. № 2. S. 75–79.

3. Primakin A.I., Sineshchuk Yu.I., Pantihovskij O.V., Sineshchuk M.Yu. Pravovye aspekty bezopasnosti edinogo informacionnogo prostranstva silovyh vedomstv (MVD, MCHS, MO) // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2012. T. 54. № 2. S. 234–240.

4. Yaroshenko A.Yu. Sistemnyj podhod k nastrojke i vnedreniyu mezhsetevyh ehkranov v gosudarstvennye informacionnye sistemy // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii. V Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferenciya: sbornik nauchnyh statej. 2016.

5. Bujnevich M.V., Izrailov K.E., Yaroshenko A.Yu., Problemnye voprosy nejtralizacii uyazvimostej programmnogo koda telekommunikacionnyh ustrojstv // Problemy upravleniya riskami v tekhnosfere. 2016. №. 3(39). C. 81–89.

6. Bujnevich, M.V., SHCHerbakov, O.V., Vladyko, A.G., Izrailov, K.E., Arhitekturnye uyazvimosti modelej telekommunikacionnyh setej // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MCHS Rossii». 2015. № 4. S. 86–93.

7. Bujnevich M.V., SHCHerbakov O.V., Izrailov K.E. Strukturnaya model' mashinnogo koda, specializirovannaya dlya poiska uyazvimostej v programmnom obespechenii avtomatizirovannyh sistem upravleniya // Problemy upravleniya riskami v tekhnosfere. 2014. № 3 (31). S. 68–74.

8. Bujnevich M.V., Izrailov K.E., SHCHerbakov O.V. Model' mashinnogo koda, specializirovannaya dlya poiska uyazvimostej // Vestnik Voronezhskogo instituta GPS MCHS Rossii. 2014. № 2 (11). S. 46–51.

9. Bujnevich M.V., Primakin A.I. Kategorial'nyj analiz problem garmonizacii normativno-pravovoj bazy informacionnoj bezopasnosti // Informacionnaya bezopasnost' regionov Rossii (IBRR-2015): materialy IX Sankt-Peterburgskoj mezhregion. konf., Sankt-Peterburg, 28–30 okt. 2015 g. SPb.: SPOISU, 2015. S. 34–35.

10. Bujnevich M.V., Vladyko A.G., Docenko S.M., Simonina O.A. Organizacionno-tekhnicheskoe obespechenie ustojchivosti funkcionirovaniya i bezopasnosti seti svyazi obshchego pol'zovaniya. SPb.: SPbGUT, 2013. 144 s.