Общие проблемы обеспечения информационной безопасности государства в современном социуме

Common problems of ensuring information security of the state in modern society

Грачев / Grachev A.
Александр Сергеевич
(gralse@mail.ru)
ФГБОУ ВО «Московский технологический университет» (Институт комплексной безопасности и специального приборостроения),
старший преподаватель.
г. Москва

Кортнев / Kortnev A.
Андрей Александрович
(kortnev.udp@gmail.com)
АО «Федеральный центр науки и высоких технологий «СНПО «Элерон»,
руководитель.
г. Москва

Лазунин / Lasunin K.
Константин Александрович
(07121917@mail.ru)
ФГБОУ ВО «Московский технологический университет» (Институт комплексной безопасности и специального приборостроения),
аспирант.
г. Москва

Ключевые слова: национальная безопасность – national security; защита информации – protection of information; информационная безопасность – information security.

В данной статье рассмотрены проблемы обеспечения информационной безопасности в современном социуме. Проведен анализ доктрины информационной безопасности и стратегии развития информационного общества Российской Федерации, с учетом положений Конституции Российской Федерации. Приведены примеры навязывания и необходимости участникам информационной системы Российской Федерации использования зарубежных программно-аппаратных технологий, ввиду отсутствия отечественных аналогов. Необходимость совершенствования профессионального кадрового потенциала в области информационной безопасности и общей компьютерной грамотности граждан Российской Федерации. Рассмотрена проблематика доверенных средств защиты информации и средств криптографической защиты информации в условиях импортозамещения. Выявлена и обоснована потребность в развитии нормативно-правовой базы по регулированию и противодействию новым вызовам и угрозам национальной безопасности.

In this article, problems of the ensuring information security (EIS) in modern society are considered. The analysis of the doctrine of information security and the development strategy of information society of the Russian Federation, taking into account provisions of the Constitution of the Russian Federation is carried out. Examples of imposing to participants of an information system of the Russian Federation of use of foreign hardware-software technologies, in a type of lack of domestic analogs are given. Need of improvement of professional personnel potential in the field of information security and the general computer literacy of citizens of the Russian Federation. The perspective of the entrusted means of information protection and means of cryptographic information security, in the conditions of import substitution is considered. The need for development of normative and legal base on regulation and counteraction to new calls and threats of national security is revealed and proved.

Состояние развития информационной безопасности [1] государства в современном социуме подразумевает защищенность ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [4]. Информационно-техническая составляющая информационной сферы [1] подразумевает использование сети глобального международного обмена интернет.

Расширение областей использования информационных технологий, являясь позитивным фактором для развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые вызовы и угрозы

национальной безопасности. Это обусловлено усиливающейся тенденцией к использованию возможностей трансграничного оборота информации в информационном пространстве для достижения геополитических, военно-политических и иных целей в ущерб международной безопасности и стратегической стабильности, а также использованием информационных технологий в террористических, криминальных и иных противоправных целях [4]. В качестве примера можно привести средства криптографической защиты информации на устройствах с недоверенными операционными системами (ОС) на недоверенной аппаратной платформе для использования гражданами Российской Федерации, являющимися участниками информационного общества, в качестве личного конфиденциального информационного обмена.

Ярким примером является внедрением агентства национальной безопасности (АНБ) закладки в генератор псевдослучайных чисел, для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ. В подтверждении данного факта, данный генератор "от АНБ" был так же сертифицирован в национальном институте стандартов и технологий (НИСТ) США [8].

Следует отметить, что в задачи АНБ должны входить эффективная организация и управление разведывательной деятельностью Соединенных Штатов в области телекоммуникаций, проводимой против иностранных правительств, с целью обеспечения целостной и действительной политики и соответствующих мер для перехвата телекоммуникаций, кроме зарубежной прессы и радиовещания, и получения информации, предназначенной для приема другим получателем, но не исключает цензуру, а также подготовку и распространение полученной информации.

Особый характер деятельности электронной разведки АНБ требует, чтобы она во всех отношениях велась отдельно от другой или общей разведывательной деятельности. Приказы, директивы, указания или рекомендации любого органа исполнительной власти, касающегося сбора, получения, защиты, обработки, распространения или использования разведывательной информации, неприменимы в отношении действий электронной разведки, если это не оговорено особо, и документы не должны издаваться без разрешения представительства агентства, входящего в правительство. Другие директивы Национального совета безопасности директору центрального разведывательного управления (ЦРУ) и связанные директивы, изданные директором ЦРУ, не должны применяться к действиям электронной разведки, если это не будет специальная директива Национального совета безопасности, касающегося электронной разведки [3].

По имеющимся данным средств массовой информации (СМИ) от 5 июня 2015 года, есть статья о том, как США позволяли АНБ без судебного решения следить за всеми международными интернет-коммуникациями американцев. Об этом пишет газета "Нью-Йорк таймс" со ссылкой на документы, переданные бывшим сотрудником спецслужбы Эдвардом Сноуденом. В материалах говориться, что в слежке за интернет-трафиком АНБ существенно превышало свои полномочия. Минюст США выдал разрешение только на мониторинг ресурсов, которые пытались взломать из-за рубежа. Агентство же выбирало цели по своему усмотрению и собирало огромные объемы данных американцев, начиная с личных писем до информации по коммерческим сделкам.

Мы можем сделать вывод о том, что общественные отношения, возникающие внутри социума в информационной сфере, определяют применения аппаратной и программной составляющей технических средств, в которой предполагается присутствие компонентов представляющих угрозу.

1. Средства защиты информации (СЗИ) и средства криптографической защиты информации (СКЗИ), как неотъемлемая часть развития информационного общества Российской Федерации.

Современные реалии говорят нам о том, что многие объекты не смогут должным образом функционировать без информационного взаимодействия с внешней средой. Крупное предприятие проблематично контролировать и обслуживать, поэтому многие административные и обслуживающие операции приходится осуществлять по удаленному доступу, что порождает массу проблем, связанных с обеспечением информационной безопасности (ОИБ).

Существует множество разработок СЗИ и СКЗИ для обеспечения безопасности информации в коммерческих целях, что в свою очередь может привести к подрыву как коммерческого сектора, так и позволит повлиять на безопасность государства. Одним из основных негативных факторов, влияющих на состояние информационной безопасности Российской Федерации, является наращивание ведущими зарубежными странами возможностей по информационно-техническому воздействию на информационную инфраструктуру для достижения своих военных целях [4].

Стоит обратить особое внимание на формирование нового подхода по рассмотрению данной проблематики, который предполагает использование недоверенной технической составляющей в информационной системе, а именно: аппаратную платформу, ПО, ОС, автоматизированную систему без подключения к глобальной международной сети интернет, однако за счет потери решения одной из основных задач о необходимости по взаимодействию между субъектами информационного поля государства. Текущее развитие инфраструктуры информационных технологий в Российской Федерации и в мире говорит о наращивании "облачных" технологий, которые в свою очередь приводят к невозможности использования в том числе и технологий межсетевого экранирования, а также систем виртуализации при

простых настройках. В таких условиях работы виртуализации невозможно осуществить категорирование систем. Это приводит к сложности работы информационной системы.

Возникает потребность объектов взаимодействия в обеспечении конфиденциальности информации. Существуют требования законодательной базы Российской Федерации о применении СКЗИ после прохождения соответствующих сертификационных испытаний в соответствии с законодательством. Одним из основных законодателей СКЗИ и работы криптографических алгоритмов является ФСБ России. Стоит поднять вопрос о внедрении отечественной доверенной аппаратной и программной среды разработок в коммерческий сектор и критически важных объектов.

2. Нехватка квалифицированного кадрового состава.

Вопросами ОИБ должен заниматься специалист по защите информации. Одной из проблем в ОИБ является человеческий фактор, стоит обратить на это внимание. Используя автоматизированные системы, подразумевающие участие человека, который, в свою очередь, является звеном, на которое может быть оказано потенциальное воздействие с целью добычи необходимой информации, а именно неправомерное получение данной информации от участника информационного обмена. В качестве примера человеческого фактора можно привести, например, системного администратора базы данных, который будет склонен к продаже доверенной информации, либо воздействие на членов семьи участников информационного взаимодействия может повлечь за собой также утечку конфиденциальной информации.

Стоит отметить, что современные подходы к информационным технологиям подразумевают ОИБ при том, что руководители организаций доверяют не своим сотрудникам, прошедшим все этапы отбора вопросов собственной безопасности, а сотрудникам другой фирмы. Примером этому может являться навязывание одной из крупнейших компаний, использовавшую технологию немецкой компании системного анализа и разработки программ SAP, который в свою очередь используется совместно с крупнейшим производителем американской компании программного обеспечения системами управления баз данных Oracle.

При возникновении технических проблем данные компании привлекают для решения этих задач иностранных граждан, а именно свой персонал, что в свою очередь будет противоречить вопросов конфиденциальности. Мы не можем гарантировать того, что допущенный сотрудник иностранного государства, имея доступ к конфиденциальной информации, не создаст утечку конфиденциальной информации. Данная проблематика требует особого внимания по совершенствованию ОИБ, которая является неотъемлемой частью в вопросе обеспечения национальной безопасности государства.

3. Курс на импортозамещение.

Отсутствие доверенных средств защиты информации и средств криптографической защиты информации в условиях отсутствия импортозамещения:

– использование иностранного программного обеспечения (ПО) может повлечь за собой отсутствие исходного кода и возложенных на него функций;

– этап сопровождения отечественной продукции менее зависим от внешнеполитической обстановки;

– наличие недекларированных возможностей в аппаратных разработках иностранной продукции;

– существует вероятность аппаратно-программных закладок реализованных под конкретную сферу деятельности. Это говорит о необходимости конфиденциальной поставке продуктов субъектам информационной сферы.

На текущий момент на предприятиях используется недоверенные аппаратные и программные технические средства, которые представляют собой серьезную угрозу для безопасности Российской Федерации.

4. Совершенствование нормативно-правового поля в сфере информационных технологий.

Тема обеспечения безопасности информации граждан влечет за собой ряд вопросов по совершенствованию нормативно-правого обеспечения, отталкиваясь от конституции по защите прав граждан. Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства [5]. Стоит обратить внимание на формирование политики информационной безопасности каждого субъекта информационной сферы, независимо коммерческого или государственного сектора. Для совершенствования безопасности необходимо пересмотреть ряд Федеральных Законов, таких как Федеральный Закон № 152 "О персональных данных", который стоит рассмотрения и доработки. Разработать Федеральный Закон "О служебной тайне". Актуальность совершенствования правового регулирования в сфере противодействия новым вызовам и угрозам национальной безопасности, их особенности, а также важная задача составляющая в обеспечении безопасности в современном мире и проблемы в вопросах борьбы с кибертерроризмом, отмечены бывшим директором ФСБ России, председателем национального антитеррористического комитета, секретарем Совета Безопасности Российской Федерации Н. П. Патрушевым [2].

Все государственные органы работают с документооборотом и в свою очередь защищены крайне плохо. На выездном совещании секретарь Совета безопасности Н. П. Патрушев отметил, что серьезную опасность представляет использование сотрудниками органами государственной власти регионов и местного самоуправления для решения служебных вопросов информационно-телекоммуникационных ресурсов, расположенных за пределами Российской Федерации. Например, сотрудниками государственной власти Хабаровского края использовались возможности целого ряда зарубежных информационно-телекоммуникационных сервисов таких как: google, yahoo, whatsapp и иных. Это является системным вопросом для всей России. В

информационных системах органов государственной власти обнаружены программные средства технических разведок [7].

Для решении данной проблемы необходим компромисс, который позволит поднять гражданский документооборот. Стоит пересмотреть нормативно-правовую базу, учитывая проблематику в государстве для обеспечения и совершенствования безопасности.

5. Недооценка угроз информационной безопасности государства.

К сожалению, многие специалисты ОИБ считают свои объекты достаточно защищенными от злонамеренных действий и не собираются выделять дополнительные затраты на ОИБ. Стоит снимать ответственность с организаций, занимающихся обеспечением защиты информации, в пользу государства, а именно формирование нестандартного подхода по обеспечению информационной безопасности. Ни для кого не секрет, что цель и задача любой коммерческой организации в повышении своего капитала и вопросы по совершенствованию и развитию сектора безопасности оказывается на втором плане. Только государство должно и может обеспечить защиту информации граждан Российской Федерации. Каждый гражданин Российской Федерации должен быть важен в целом. Не стоит забывать, что защита от вмешательства в частную жизнь, является задачей государства. Влияние на Российскую Федерацию через граждан иностранными спецслужбами по средствам внедрения технических средств влечет за собой угрозу Российской Федерации. В стратегию развития информационного общества в Российской Федерации входит обеспечение национальной безопасности в информационной сфере [6].

Применение своей доверенной программной реализации на недоверенной аппаратной платформе с использованием аппаратно реализуемых методов шифрования по ГОСТ позволит подойти к решению выше указанных проблем и стать одним из направлений по развитию целой области в вопросах защиты в условиях всего недоверенного. Стоит подойти к созданию доверенного ПО, а именно полной замене программного кода в случае использования недоверенного, на низком уровне восприятия команд процессора аппаратного устройства. При этом речь идет о создании ОС на низком уровне программирования и наращивании отраслевого потенциала государства, за счет отказа отсистемы автоматизированной разработки ПО всеми известными языками программирования.

Применение метода по формированию подхода обеспечения информационной безопасности с использованием доверенной отечественной аппаратной и программной среды является актуальным решением проблемы защиты информации в обеспечении национальной безопасности.

Литература

1. Масановец, В. В. Методы комплексного контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления: Монография / В.В. Масановец, А.П. Фесун, О.Г. Никифоров ; под общей редакцией В.В. Масановца. – М.: Управление делами Президента Российской Федерации, 2009. – 368 с.

2. Патрушев, Н. П. Особенности современных вызовов и угроз национальной безопасности России / Н.П. Патрушев // Журнал российского права. – 2007. – № 7 (127). – С. 3–12.

3. Truman, H. Memorandum for: The Secretary of State, The Secretary of Defense / H. Truman. A 207075/4/54/OSO, NSA TS CONTL. NO 73-00405, 24 Oct 1952.

4. Указ Президента Российской Федерации от 05.12.2016 г. № 646 [Электронный ресурс] // Сайт Администрации Президента Российской Федерации, 2016. – Режим доступа: http://kremlin.ru/acts/bank/41460 , свободный. – Загл. с экрана.

5. Конституция Российской Федерации [Электронный ресурс] // Сайт Администрации Президента Российской Федерации, 1993. – Режим доступа: http://constitution.kremlin.ru, свободный. – Загл. с экрана.

6. Указ Президента Российской Федерации от 09.05.2017 г. № 203 [Электронный ресурс] // Сайт Администрации Президента Российской Федерации, 2017. – Режим доступа: http://kremlin.ru/acts/bank/41919, свободный. – Загл. с экрана.

7. Доклад секретаря Совета безопасности Патрушева Н. П. [Электронный ресурс] // Сайт ТАСС информационного агентства Российской Федерации, 2015. – Режим доступа: http://tass.ru/politika/2211260, свободный. – Загл. с экрана.

8. Специальная публикация о сертификации генератора случайных чисел (Special Publication 800-90A) [Электронный ресурс] // Сайт государственного национального института стандартов и технологий США, 2012. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf, свободный. – Загл. с экрана.