ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК: 332.1
JEL: R1, O11. O33, O40

Создание единой системы противодействия кибератакам: ответ на большие вызовы и угрозы налоговой безопасности страны

Т.В. Деева, к.ю.н., докторант ИПР РАН
e-mail: *tv_k@lenta.ru*

Аннотация
Предмет/тема. Предметом исследования статьи является процесс создания единой системы противодействия кибератакам в целях обеспечения налоговой безопасности страны. ***Цели/задачи.*** Целью данной статьи является исследование основ создания единой системы противодействия кибератакам в ответ на большие вызовы и угрозы налоговой безопасности страны. ***Методология*** исследования включает методы правового и логического анализа. ***Результаты.*** На основе проведенного нами анализа нормативной правовой базы определено назначение и ключевые задачи Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Также автором конкретизированы приоритетные направления информатизации фискальной службы на современном этапе на примере АИС «Налог-3». Рассмотрены основные угрозы информационной безопасности налоговых органов. Представлены задачи и архитектура модуля СОБИ АИС «Налог-3», позволяющего достичь требуемого уровня защищенности информационных ресурсов системы и оперативного реагирования на возникающие угрозы безопасности информации. Определены основы взаимодействия ФНС и ФСБ в области противодействия кибератакам. ***Выводы/значимость.*** Для того чтобы повысить уровень устойчивости национальных информационных ресурсов в условиях кибератак была создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Взаимодействие ФНС с данной системой направлено на решение такой совокупности задач: выявление причин, по которым происходят компьютерные инциденты в информационных ресурсах ФНС России; организация контроля степени защищенности информационных ресурсов ФНС России; обеспечение продуктивного межведомственного взаимодействия между ФНС России и ФСБ России; прогнозирование ситуаций в области информационной безопасности налоговых органов.

Ключевые слова: *ГосСОПКА, СОБИ АИС «Налог-3», кибератаки, сетевые атаки, киберугрозы, кибербезопасность*

DOI: https://doi.org/10.33051/2500-2325-2020-4-100-112

Введение

Актуальность выбранной темы данной статьи обусловлена тем, что основным трендом развития государства в настоящее время является внедрение цифровой экономики. В то же время, преимущества современного цифрового мира и развитие информационных технологий обусловили возникновение новых угроз национальной и международной безопасности.

В условиях глобализации информационных процессов, их интеграции в разные сферы общественной жизни руководство ведущих государств мира усиливает внимание созданию и усовершенствованию эффективных систем как киберзащиты, так и кибербезопасности объектов критической инфраструктуры от внешних и внутренних угроз кибернетического характера.

В последнее время проблема обеспечения безопасности смещается в сторону не столько декларируемой, сколько реально рассматриваемой. Для любого государства на всех этапах его

развития вопрос безопасности является ключевым. Во многих ведущих странах мира уже сформированы общегосударственные (национальные) системы кибернетической безопасности – как наиболее оптимальные организационно-функциональные структуры, способные в короткий промежуток времени аккумулировать силы и средства компетентных органов государственной власти с привлечением общественных структур для противодействия киберугрозам различного характера (киберинциденты, кибератаки, киберпреступления). Это связано преимущественно с национальными интересами, которые во все времена нуждаются в серьезном отношении власти и общества.

Несмотря на распространенность кибератак в современном обществе, в Российской Федерации отсутствует надлежащее законодательное обеспечение, которое бы регламентировало отношения в данной сфере.

Обзор литературы

Государство – это система правовых институтов, обеспечивающих скоординированные действия отдельных индивидов и бизнеса по достижению общей цели.

В ходе исследования трактовки сущности и содержания дефиниции «налоговая безопасность» было установлено, что среди ученых и исследователей доминирует понимание ее экономико-правовой формы [11], что обеспечивает создание государством условий для взаимодействия интересов личности, предпринимательских структур и государства на основе соблюдения принципа взаимной ответственности субъектов налогообложения.

Налоги, которые поступают в бюджет, формируют финансовую основу для развития государства. Существует такое понятие, как налоговая безопасность. Она является неотъемлемой частью экономической безопасности и ее следует рассматривать как интегрированную подсистему финансовой безопасности.

Большая значимость налоговой составляющей части для функционирования национальной экономики и формирования экономической безопасности, по нашему мнению, является аргументом, что она выходит за пределы обеспечения финансовой безопасности и может быть выделена как отдельный элемент системы экономической безопасности в целом.

Процесс управления в налоговых органах невозможен без накопления соответствующей информации. Без надлежащей информации трудно провести необходимую оценку соответствующей ситуации, выявить имеющиеся проблемы, предусмотреть возможный ход действий, сформировать цели, которых нужно достичь, выработать и утвердить определенные решения по управлению этими процессами и выполнить контроль за их реализацией.

Информационная безопасность предусматривает действенный комплекс мер, которые должны надежно защищать финансово-экономическую, социальную, политическую и другие сферы деятельности государства, интеллектуальную собственность лиц, а также сведения, составляющие предусмотренную законом тайну.

Как показал анализ литературы[1], именно внедрение современных информационных технологий в электронные системы управления, оборонного, экономического и других секторов экономики ведущих стран мира обусловило усиление зависимости безопасного функционирования этих систем от внешнего кибернетического воздействия. При таких обстоятельствах проблемы обеспечения кибернетической безопасности любой страны приобретают важное значение и требуют от руководства государства внедрения комплекса нормативно-правовых и организационных мер, направленных на наращивание возможностей защиты национального киберпространства.

Большинство угроз информационной безопасности ФНС России сопряжено с несанкционированным доступом в целях ознакомления, копирования, изменения, распространения дан-

[1] National Cybersecurity Protection Act of 2014. [Электронный ресурс]. – URL: https://www.congress.gov/bill/113th-congress/senate-bill/2519/text (Дата обращения: 12.08.2020); Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2 / 2012. [Электронный ресурс]. – URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Дата обращения: 12.08.2020).

ных, либо деструктивного воздействия на информационную систему, ее отдельные элементы и обрабатываемую информацию[2].

Важным направлением исследований и теоретиков, и практиков остается вопрос применения передовых информационных технологий в государственном управлении, изучение ведомственных информационных систем для дальнейшей их интеграции в единую инфраструктуру государственных органов страны. Особенно актуален вопрос использования информационно-коммуникативных технологий (далее – ИКТ) налоговыми органами в процессе трансформации фискальной службы в сервисную, переход на электронный формат взаимодействия налогоплательщиков и налоговых органов. В статьях Маликовой К.Р., Алимирзоевой М.Г. [16], Гарифуллиной Г.В. [12], Филипповой Н.А., Сергачевой Т.В. [18] рассматриваются вопросы информационной трансформации и внедрения информационной системы АИС «Налог-3» в деятельность налоговых органов.

В исследованиях Яблокова Д.Ю. [20], Костенковой О.М. [14] обсуждаются вопросы обеспечения безопасности в АИС «Налог-3». Автор данной статьи согласен с другими исследователями, что характерными чертами информационной безопасности в налоговых органах Российской Федерации являются: обеспечение безопасности доступности комбинаций, целостности и конфиденциальности информационных баз данных.

Множество статей современных исследователей посвящены вопросам обеспечения кибербезопасности. Так, Калмыков В.В. [13], Лобач Д.В., Смирнова Е.А. [15] в своих статьях рассматривают вопросы, связанные с реализацией политики государства в обеспечении информационной безопасности в РФ. Авторами проанализированы современные механизмы обеспечения информационной безопасности, определенные в Доктрине информационной безопасности РФ[3]. Анализ проводится на примере ГосСОПКА. Разработка этой системы началась специалистами ФСБ России в 2013 г. по поручению Президента РФ Владимира Владимировича Путина[4]. Цели системы – выявление, предупреждение и ликвидация последствий хакерских компьютерных атак на информационные ресурсы, располагающиеся на территории РФ, в консульских учреждениях и дипломатических представительствах России за границей[5].

Основными задачами создания ГосСОПКА выступают:

1. Задача по обеспечению условий, в которых субъекты КИИ смогут полноценно взаимодействовать между собой.

2. Задача по прогнозированию перспектив в области информационной безопасности.

3. Задача по установлению и предотвращению причин, обусловливающих инциденты в кибер-сфере.

4. Задача по установлению контроля с целью обеспечения защищенности информационных ресурсов.

Федеральным органом исполнительной власти, уполномоченным на создание ГосСОПКА, выступает Федеральная служба безопасности (ФСБ России).

Задачи, поставленные перед системой ГосСОПКА, должны решаться во всем информационном пространстве России путем осуществления взаимодействия со всеми субъектами, владеющими ресурсами в информационном пространстве, кто ответственно относится как к без-

[2] Приказ ФНС России от 25.02.2014 № ММВ-7-6/66@ (ред. от 19.06.2018) «Об утверждении Концепции системы управления информационной безопасностью ФНС России».

[3] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

[4] Указ Президента РФ от 15.01.2013 № 31с (ред. от 22.12.2017) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»; Указ Президента РФ № К 1274 от 12.12.2014 «О Концепции ГосСОПКА»; Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

[5] Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА. [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/ (Дата обращения: 12.08.2020).

опасности собственных ресурсов, так и к безопасности информационного пространства в целом[6]. Взаимодействие может осуществляться в разных формах:

а) в форме информационного обмена, когда субъекты обмениваются данными о новых рисках, угрозах и компьютерных инцидентах;

б) в форме сотрудничества, при котором субъектами решаются задачи по выявлению, регистрации, реагированию и устранению риска компьютерных инцидентов.

Согласно действующему законодательству, обязанность взаимодействовать с ГосСОПКА и объединять средства с целью выявления, предупреждения и ликвидации кибератак[7] предусмотрена исключительно для субъектов КИИ, то есть для ИП, юридических лиц и государственных органов, заключивших соглашения с ФСБ России.

Сотрудничество с ГосСОПКА обеспечивается благодаря деятельности Национального координационного центра по компьютерным инцидентам (НККЦКИ). Центр занимается:

а) сбором и обменом сведениями об инцидентах между субъектами критической инфраструктуры;

б) представлением методических рекомендаций по предупреждению кибератак;

в) координацией мероприятий по реагированию[8].

Результаты исследования

Развитие и безопасность информационных ресурсов органов ФНС России, внедрение электронного управления, обеспечение безопасности и устойчивого функционирования электронных коммуникаций и государственных электронных информационных ресурсов должны быть составляющими государственной политики в сфере развития информационного пространства и становления информационного общества в России.

Основным информационным ресурсом налоговых органов, который используют во время текущей деятельности сотрудники, выступает АИС «Налог-3»[9], благодаря которой обеспечивается объединение и структурирование разрозненных налоговых данных в единую БД. Единая система противодействия кибератакам в ФНС сформирована с целью обеспечения централизованной технической и организационной политики по обеспечению безопасности информации автоматизированной информационной системы «Налог-3». В декабре 2018 г. ФНС России интегрировала потоки данных из онлайн-касс, системы прослеживаемости и маркировки товаров, а также из АИС «Налог-3» в единую информационную мегасистему, функционирующую на базе Big Data[10].

Применение современных средств информационного обеспечения в управленческих технологиях государственных органов значительно упрощает процедуры, которые осуществляют фискальные органы; положительно влияет на качество их операционной деятельности и при таких условиях генерирует современную информационную инфраструктуру ФНС России. Кроме вышеупомянутых средств информатизации управленческих процессов, составляющими инфраструктуры являются информационные продукты налогового сервиса, от качества и количе-

---

[6] Качалин И.Ф. Роль и назначение ГосСОПКА в современной системе информационной безопасности Российской Федерации. [Электронный ресурс]. – URL: https://soc-forum.ib-bank.ru/files/files/SOC%202018/01_kachalin.pdf (Дата обращения: 12.08.2020).

[7] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция).

[8] Нормативные документы в области ГосСОПКА и безопасности КИИ. [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/terminology-gossopka-kii-full-version/ (Дата обращения: 12.08.2020); Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам».

[9] Приказ Федеральной налоговой службы от 14 марта 2016 г. № ММВ-7-12/134@ «Об утверждении Положения об автоматизированной информационной системе Федеральной налоговой службы (АИС «Налог-3»)».

[10] Какие технологии будет использовать ФНС через 5-10 лет? // Генеральный директор. – 2019. – № 4. [Электронный ресурс]. – URL: https://www.gradient-alpha.ru/kakie-tekhnologii-budet-ispolzovat/ (Дата обращения: 12.08.2020).

ства которых также зависит эффективность государственного управления налогообложением [20].

Основные угрозы информационной безопасности налоговых органов, определенные в Концепции информационной безопасности ФНС, представлены на рис. 1 и включают: иностранные технические разведки, терроризм, хакеров (компьютерных злоумышленников), производителей и пользователей программного обеспечения налоговой службы и др. По мнению автора, также важным фактором угрозы информационной безопасности налоговых органов являются кибератаки, осуществляемые с целью определение уровня устойчивости инфраструктуры Российской Федерации.

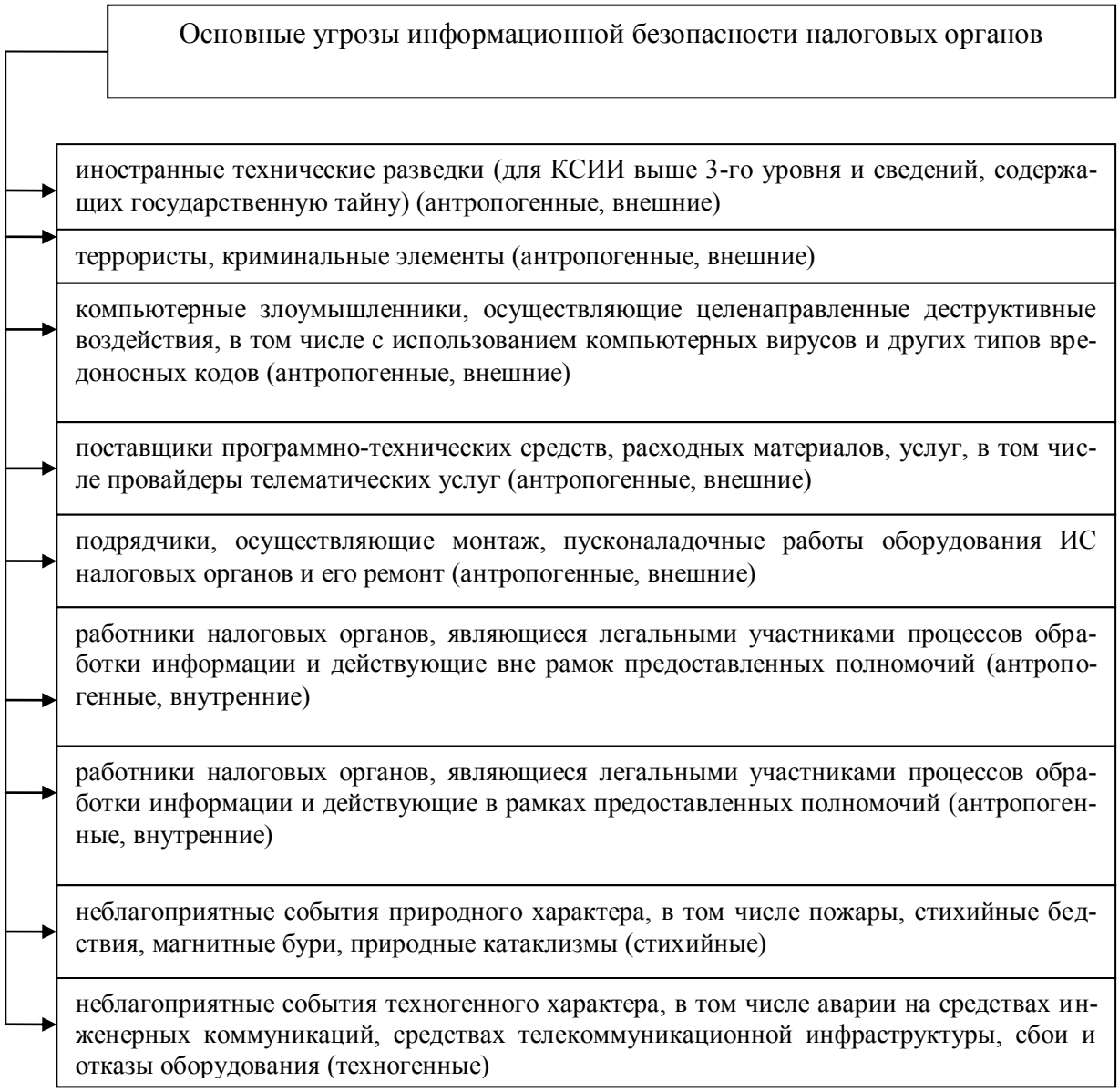

Рис. 1. Основные угрозы информационной безопасности налоговых органов[11].

Для обеспечения информационной безопасности и нивелирования указанных угроз в АИС «Налог-3» функционирует модуль СОБИ, который представляет собой объединение четко

[11]Составлено автором на основе: Приказ ФНС России от 13.01.2012 № ММВ-7-4/6@ «Об утверждении Концепции информационной безопасности Федеральной налоговой службы».

регламентированных организационных мероприятий, которыми устанавливаются правила доступа, обработки и использования защищаемых данных. Благодаря системе СОБИ АИС «Налог-3» обеспечивается достижение необходимого уровня защищенности ресурсов информационной системы. Кроме того, появляется возможность оперативного реагирования на угрозы безопасности данных и негативные тенденции роста этих угроз[12]. СОБИ в АИС «Налог-3» состоит из двух составляющих – пассивной и активной [14]. Задачи СОБИ АИС «Налог-3» представлены на рис. 2.

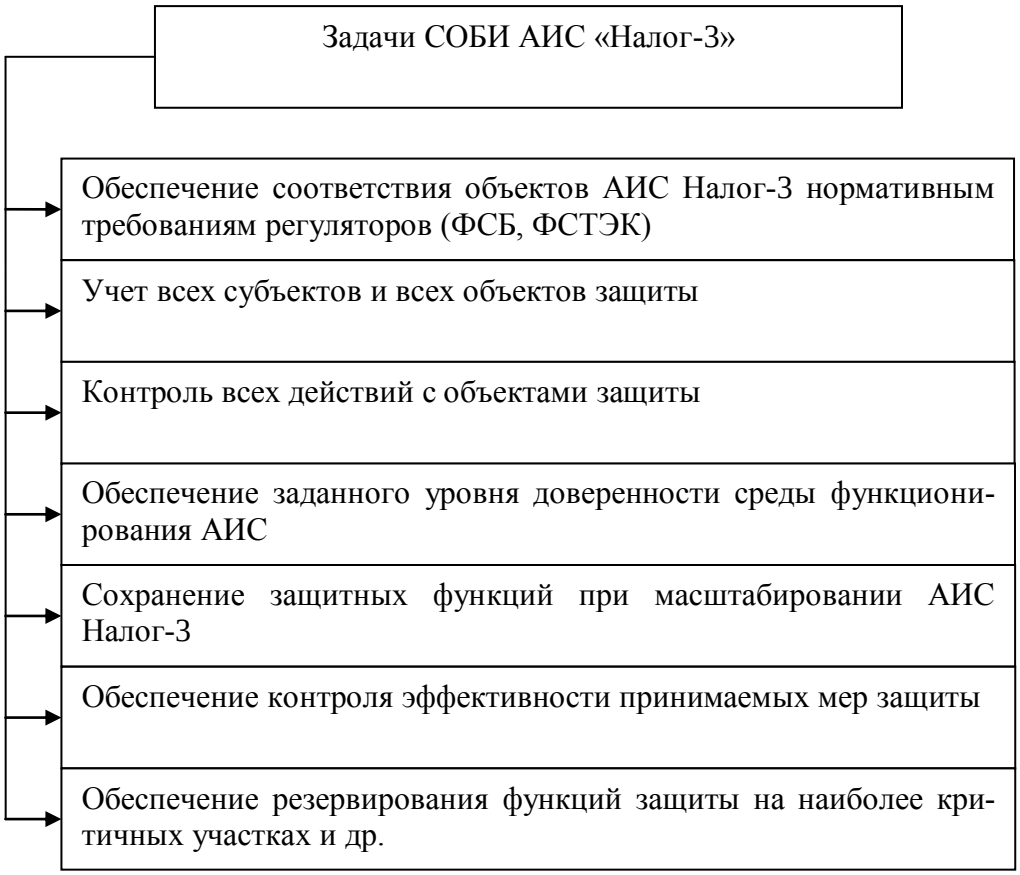

Рис. 2. Задачи СОБИ АИС «Налог-3»[13].

Архитектура СОБИ АИС «Налог-3» содержит несколько модулей: организационная база, исполнительный механизм, механизм поддержки. Общая архитектура СОБИ АИС «Налог-3» представлена на рис. 3.

[12] Мухортов Ю.В. Комплексные решения вопросов обеспечения безопасности информации для государственных информационных систем (на примере построения СОБИ АИС «НАЛОГ-3»). [Электронный ресурс]. – URL: https://elvis.ru/upload/iblock/702/mukhortov_fns.pdf (Дата обращения: 12.08.2020).

[13] Составлено автором на основе: Мухортов Ю.В. Комплексные решения вопросов обеспечения безопасности информации для государственных информационных систем (на примере построения СОБИ АИС «НАЛОГ-3»). [Электронный ресурс]. – URL: https://elvis.ru/upload/iblock/702/mukhortov_fns.pdf (Дата обращения: 12.08.2020).

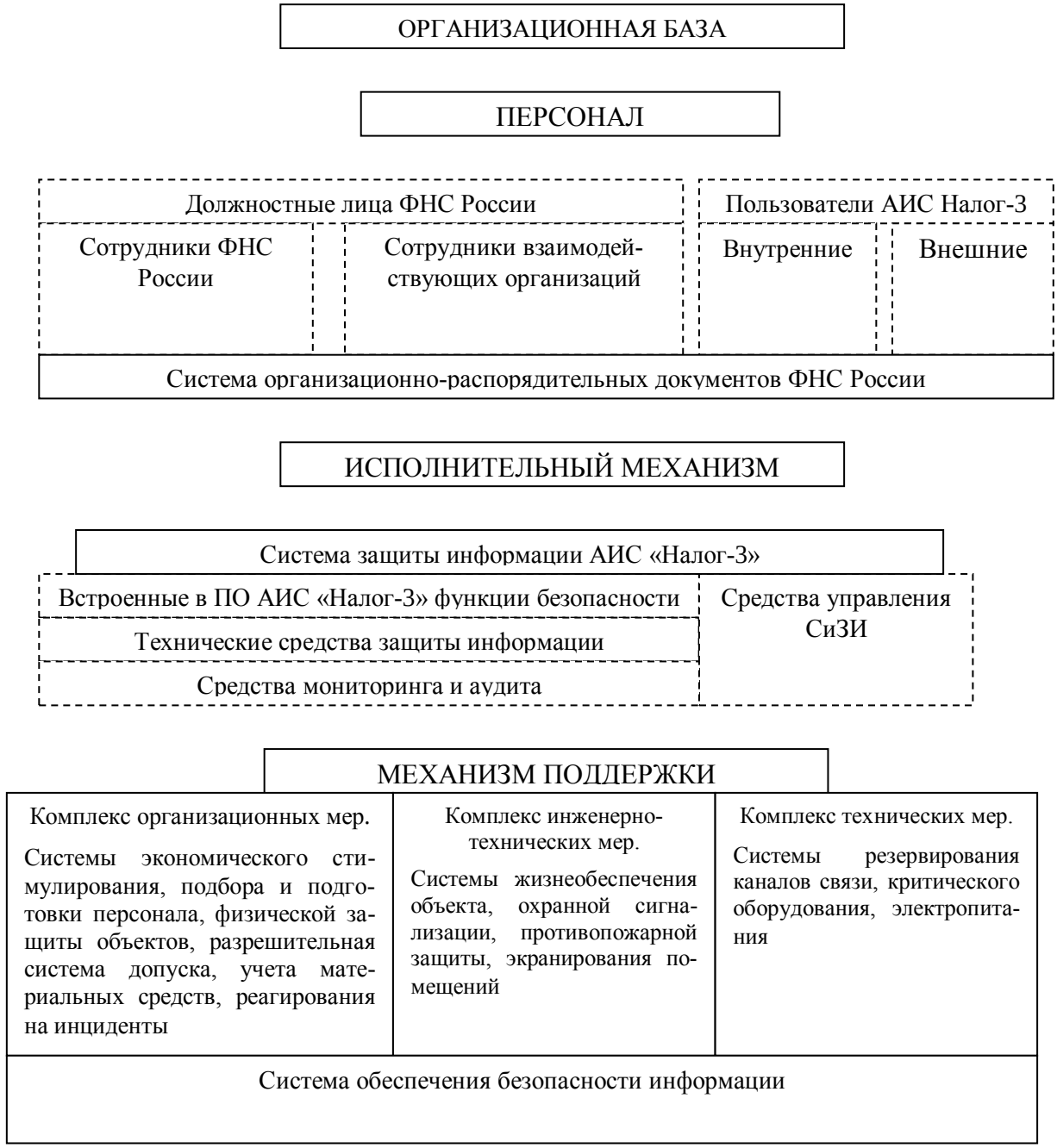

Рис. 3. Общая архитектура СОБИ АИС «Налог-3»[14].

Для развития системы налоговой безопасности и внесения в нее изменений необходимо следующее:

1. Во-первых, нужно создать соответствующие информационные технологии.
2. Во-вторых, необходимо повысить научно-технический потенциал.
3. В-третьих, должны быть усовершенствованы информационные и аналитические системы, а также системы прогнозирования и анализа в налоговых органах.
4. В-четвертых, нужно модернизировать систему учета плательщиков налогов и сборов, а также систему учета платежей.

[14] Мухортов Ю.В. Комплексные решения вопросов обеспечения безопасности информации для государственных информационных систем (на примере построения СОБИ АИС «НАЛОГ-3»). [Электронный ресурс]. – URL: https://elvis.ru/upload/iblock/702/mukhortov_fns.pdf (Дата обращения: 12.08.2020).

Необходимо отметить что, система СОБИ АИС «Налог-3» не позволяет обеспечить полную защиту ФНС от кибератак. ФНС заключает контракты с ГосСОПКА на обеспечение бесперебойной работы информационных систем и поддержание в актуальном состоянии способности данных систем реагированию на современные угрозы, и дальнейшего наращивания функциональных возможностей.

Согласно положениям Приказа ФСБ России от 19.06.2019 № 282[15], в рамках осуществления взаимодействия ФНС России как КИИ должен проинформировать ФСБ России обо всех компьютерных инцидентах, связанных с функционированием принадлежащих ему:

– значимых объектов критической информационной инфраструктуры – на протяжении трех часов с момента выявления компьютерного инцидента;

– незначимых объектов критической информационной инфраструктуры – на протяжении суток с момента, когда был выявлен компьютерный инцидент.

Данные передаются ФНС России через НКЦКИ одним из следующих способов:

– с использованием технической инфраструктуры НКЦКИ;

– по телефону;

– по факсу;

– с сайта cert.gov.ru.

Имеющимся и потенциальным угрозам, связанным с информационной безопасностью, надо предоставить статус самых серьезных проблемных вопросов XXI века. Это можно объяснить тем, что через научно-технический прогресс и новые информационно-коммуникационные технологии угрозы являются производными от многочисленных источников, а их главным проявлением выступает подрывная деятельность, целями которой становятся физические и юридические лица, национальная инфраструктура и правительства.

Современные методы, направленные на обработку, передачу и накопление информации, вызвали возникновение угроз, связанных с возможной потерей, искажением и раскрытием информации, которой обладают конечные потребители, в том числе, государство. То есть разнообразные операции с информацией имеют влияние на возникновение угроз информационной безопасности национального уровня. От того, какими будут состояние и уровень противодействия информационным вызовам, зависит и уровень государственной информационной безопасности.

Для дальнейшего совершенствования информационного обеспечения управления в налоговых органах нужно провести действенные мероприятий, которые проявятся в следующем:

– в организации защиты налоговыми органами конфиденциальной информации о физических и юридических лицах для недопущения несанкционированного распространения такой информации, а также обеспечении высокого уровня администрирования налогов, сборов, обязательных платежей;

– в разработке специальных программных комплексов для выявления и противодействия несанкционированному вмешательству в информационно-телекоммуникационные системы налоговых органов;

– в осуществлении систематического анализа налоговых рисков, которые могут быть связаны с несанкционированным вмешательством в работу автоматизированных систем налоговых органов России, с целью оперативного реагирования и координации деятельности структурных подразделений по их отработке;

– в выполнении аналитической работы соответствующими подразделениями налоговых органов для определения фактов противоправной деятельности в налоговой сфере.

[15] Приказ ФСБ России от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».

Выводы

Основными комплексными мероприятиями по защите информации и информационных отношений в ФНС являются: специальное делопроизводство; режим секретности, включая техническую защиту информации; техническая и криптографическая защита информации; голографическая защита носителей информации; правовая и организационная защита информации как обособленные виды защиты, предусматривающие порядок защиты, юридическую ответственность, так и составляющие всех других видов.

Основным информационным ресурсом ФНС является информационная система АИС «Налог-3», для обеспечения информационной безопасности которой создан модуль СОБИ АИС «Налог-3». Данный модуль не позволяет осуществлять эффективное противодействие компьютерным атакам.

Для того чтобы повысить уровень устойчивости национальных информационных ресурсов в условиях кибератак была создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Взаимодействие ФНС с данной системой направлено на решение такой совокупности задач:

– выявление причин, по которым происходят компьютерные инциденты в информационных ресурсах ФНС России;

– организация контроля степени защищенности информационных ресурсов ФНС России;

– обеспечение продуктивного межведомственного взаимодействия между ФНС России и ФСБ России;

– прогнозирование ситуации в области информационной безопасности налоговых органов.

Литература

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция).

2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

3. Указ Президента РФ от 15.01.2013 № 31 с (ред. от 22.12.2017) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

4. Указ Президента РФ № К 1274 от 12.12.2014 «О Концепции ГосСОПКА».

5. Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

6. Приказ ФНС от 14 марта 2016 г. № ММВ-7-12/134@ «Об утверждении Положения об автоматизированной информационной системе Федеральной налоговой службы (АИС «Налог-3»)».

7. Приказ ФНС России от 13.01.2012 № ММВ-7-4/6@ «Об утверждении Концепции информационной безопасности Федеральной налоговой службы».

8. Приказ ФНС России от 25.02.2014 № ММВ-7-6/66@ (ред. от 19.06.2018) «Об утверждении Концепции системы управления информационной безопасностью ФНС России»

9. Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам».

10. Приказ ФСБ России от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».

11. Варакса Н.Г. Налоговая безопасность в структуре национальной безопасности страны // Экономические и гуманитарные науки. – 2013. – № 12 (263). – С. 97-100.

12. Гарифуллина Г.В. Это реализация инновационных проектов службы–внедрение АИС «Налог-3» // В сборнике: Совершенствование налогового администрирования. Материалы первой научно-практической конференции. – 2016. – С. 72-78.

13. Калмыков В.В. Государственная политика противодействия современным стратегиям информационных войн в рамках новой доктрины информационной безопасности Российской Федерации // Ученые записки. – 2017. – № 2 (22). – С. 6-9.

14. Костенкова О.М. АИС «Налог-3» как основная информационная система налоговых органов России // Аллея науки. – М.: Издательский дом «Quantum». – 2018. – Том 1. – № 5 (21). – С. 633-637.

15. Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2019. – Т. 11. – № 4. – С. 23-32.

16. Маликова К.Р., Алимирзоева М.Г. Использование автоматизированной информационной системы АИС «Налог-3» в деятельности налоговых органов // В сборнике: Совершенствование налогообложения как фактор экономического роста. Материалы VII Международной научно-практической конференции. – 2015. – С. 21-24.

17. Смоленцева Е.В. Налоговая безопасность как составная часть финансовой безопасности страны // Успехи современной науки и образования. – 2017. – Т. 3. – № 2. – С. 175-177.

18. Филиппова Н.А., Сергачева Т.В. Оценка условий и результатов внедрения АИС «Налог-3» в налоговых органах региона // Регионология. – 2017. – Т. 25. – № 1 (98). – С. 79-91.

19. Цветков В.А., Дудин М.Н., Лясников Н.В., Зоидов К.Х. Система налогового контроля в Российской Федерации и пути повышения ее эффективности // Экономика и управление. – 2019. – № 1 (159). – С. 4-15.

20. Яблоков Д.Ю. Обеспечение безопасности процедур в системе электронного налогового администрирования // Финансы и управление. – 2018. – № 3. – С. 19-27.

21. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак ГосСОПКА. [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/ (Дата обращения: 12.08.2020).

22. Мухортов Ю.В. Комплексные решения вопросов обеспечения безопасности информации для государственных информационных систем (на примере построения СОБИ АИС «НАЛОГ-3»). [Электронный ресурс]. – URL: https://elvis.ru/upload/iblock/702/mukhortov_fns.pdf (Дата обращения: 12.08.2020).

23. Нормативные документы в области ГосСОПКА и безопасности КИИ. [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/terminology-gossopka-kii-full-version/ (Дата обращения: 12.08.2020).

24. National Cybersecurity Protection Act of 2014. [Электронный ресурс]. – URL: https://www.congress.gov/bill/113th-congress/senate-bill/2519/text (Дата обращения: 12.08.2020).

25. Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2 / 2012 / [Электронный ресурс]. – URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Дата обращения: 12.08.2020).

Об авторе

Деева Татьяна Владимировна, кандидат юридических наук, докторант, Институт проблем рынка РАН, Москва.

Для цитирования

Деева Т.В. Создание единой системы противодействия кибератакам: ответ на большие вызовы и угрозы налоговой безопасности страны // Проблемы рыночной экономики. – 2020. – № 4. – С. 100-112.

DOI: https://doi.org/10.33051/2500-2325-2020-4-100-112

Creation of a unified system of countering cyber attacks: response to major challenges and threats to the country's tax security

Tatyana V. Deeva, Cand. of Sci (Law.), Doctoral candidate
e-mail: *tv_k@lenta.ru*

Abstract

The subject/topic. The subject of the article is the process of creating a unified system of countering cyber attacks in order to ensure the tax security of the country. ***Goals/objectives***. The purpose of this article is to study the foundations of creating a unified system of countering cyber attacks in response to major challenges and threats to the country's tax security. The research methodology includes methods of legal and logical analysis. ***Results.*** Based on our analysis of the regulatory legal framework, the purpose and key tasks of the State System for Detection, Prevention and Elimination of the Consequences of Computer Attacks (GosSOPKA) have been determined. The author also concretized the priority directions of informatization of the fiscal service at the present stage using the example of AIS «Tax-3». The main threats to information security of tax authorities are considered. The article presents the tasks and architecture of the SOBI AIS «Tax-3» module, which allows to achieve the required level of security of information resources of the system and prompt response to emerging threats to information security. The basics of interaction between the Federal Tax Service and the FSB in the field of countering cyber attacks have been determined. ***Conclusions/Relevance.*** In order to increase the level of sustainability of national information resources in the face of cyber attacks, the State System for Detection, Prevention and Elimination of the Consequences of Computer Attacks (GosSOPKA) was created. Interaction of the Federal Tax Service with this system is aimed at solving such a set of tasks: identifying the reasons why computer incidents occur in the information resources of the Federal Tax Service of Russia; organization of control over the degree of protection of information resources of the Federal Tax Service of Russia; ensuring productive interagency interaction between the Federal Tax Service of Russia and the FSB of Russia; forecasting the situation in the field of information security of tax authorities.

Keywords*:* *GosSOPKA, SOBI AIS «Tax-3», cyber attacks, network attacks, cyber threats, cyber security*

References

1. Federal Law «On the Security of Critical Information Infrastructure of the Russian Federation» dated July 26, 2017 No. 187-FZ (last edition). (In Russian).

2. Decree of the President of the Russian Federation of 05.12.2016 No. 646 «On approval of the Doctrine of information security of the Russian Federation». (In Russian).

3. Decree of the President of the Russian Federation of January 15, 2013 No. 31s (as amended of December 22, 2017) «On the creation of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation». (In Russian).

4. Decree of the President of the Russian Federation No. K 1274 dated 12.12.2014 «On the Concept of the State System of Public Administration of Public Domains». (In Russian).

5. Decree of the President of the Russian Federation of December 22, 2017 No. 620 «On improving the state system for detecting, preventing and eliminating the consequences of computer attacks on the information resources of the Russian Federation». (In Russian).

6. Order of the Federal Tax Service dated March 14, 2016 No. MMB-7-12 / 134 @ «On approval of the Regulations on the automated information system of the Federal Tax Service (AIS «Tax-3»)». (In Russian).

7. Order of the Federal Tax Service of Russia dated 13.01.2012 No. MMB-7-4 / 6 @ «On Approval of the Concept of Information Security of the Federal Tax Service». (In Russian).

8. Order of the Federal Tax Service of Russia dated February 25, 2014 No. MMB-7-6 / 66 @ (as amended on June 19, 2018) «On Approval of the Concept of the Information Security Management System of the Federal Tax Service of Russia». (In Russian).

9. Order of the FSB of Russia dated July 24, 2018 No. 366 «On the National Coordination Center for Computer Incidents». (In Russian).

10. Order of the FSB of Russia dated June 19, 2019 No. 282 «On approval of the Procedure for informing the FSB of Russia about computer incidents, responding to them, taking measures to eliminate the consequences of computer attacks carried out against significant objects of the critical information infrastructure of the Russian Federation». (In Russian).

11. Varaksa N.G. Tax security in the structure of national security of the country // Economic and humanitarian sciences. – 2013. – No. 12 (263). – Pp. 97-100. (In Russian).

12. Garifullina G.V. This is the implementation of innovative projects of the service the introduction of the AIS «Tax-3» // In the collection: improving tax administration. Materials of the first scientific and practical conference. – 2016. – Pp. 72-78. (In Russian).

13. Kalmykov V.V. State policy of countering modern strategies of information wars within the framework of the new doctrine of information security of the Russian Federation // Uchenye zapiski. – 2017. – No. 2 (22). – Pp. 6-9. (In Russian).

14. Kostenkova O.M. AIS «Tax-3» as the main information system of the tax authorities of Russia // Alley of Science. – M.: «Quantum» publishing house. – 2018. – Vol. 1. – No. 5 (21). – Pp. 633-637. (In Russian).

15. Lobach D.V., Smirnova E.A. The state of cybersecurity in Russia at the present stage of the digital transformation of society and the formation of a national system for countering cyber threats // Territory of new opportunities. Bulletin of the Vladivostok State University of Economics and Service. – 2019. – Vol. 11. – No. 4. – Pp. 23-32. (In Russian).

16. Malikova K.R., Alimirzoeva M.G. The use of the automated information system AIS «Tax-3» in the activities of tax authorities // In the collection: Improving taxation as a factor of economic growth. Materials of the VII International Scientific and Practical Conference. – 2015. – Pp. 21-24. (In Russian).

17. Smolentseva E.V. Tax security as an integral part of the country's financial security // Successes of modern science and education. – 2017. – Vol. 3. – No. 2. – Pp. 175-177. (In Russian).

18. Filippova N.A., Sergacheva T.V. Assessment of the conditions and results of the introduction of AIS «Tax-3» in the tax authorities of the region // Regionology. – 2017. – Vol. 25. – No. 1 (98). – Pp. 79-91. (In Russian).

19. Tsvetkov V.A., Dudin M.N., Lyasnikov N.V., Zoidov K.Kh. Tax control system in the Russian Federation and ways to improve its efficiency // Economics and Management. – 2019. – No. 1 (159). – Pp. 4-15. (In Russian).

20. Yablokov D.Yu. Ensuring the safety of procedures in the system of electronic tax administration // Finance and Management. – 2018. – No. 3. – Pp. 19-27. (In Russian).

21. State system of detection, prevention and elimination of the consequences of computer attacks GosSOPKA. [Electronic resource]. – URL: https://www.tadviser.ru/index.php/ (Access date: 12.08.2020, In Russian).

22. Mukhortov Yu.V. Complex solutions for information security issues for state information systems (on the example of building SOBI AIS «Tax-3»). [Electronic resource]. – URL: https://elvis.ru/upload/iblock/702/mukhortov_fns.pdf (Access date: 12.08.2020, In Russian).

23. Normative documents in the field of GosSOPKA and KII security. [Electronic resource]. – URL: https://www.ptsecurity.com/ru-ru/research/knowledge-base/terminology-gossopka-kii-full-version/ (Access date: 12.08.2020, In Russian).

24. National Cybersecurity Protection Act of 2014. [Electronic resource]. – URL: https://www.congress.gov/bill/113th-congress/senate-bill/2519/text (Access date: 12.08.2020, In English).

25. Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2 / 2012. [Electronic resource]. – URL:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Access date: 12.08.2020, In English).

About author

Tatyana V. Deeva, Candidate of Sci (Law.), Doctoral candidate, Market Economy Institute of RAS, Moscow.

For citation

Deeva T.V. Creation of a unified system of countering cyber attacks: response to major challenges and threats to the country's tax security // Market economy problems. – 2020. – No. 4. – Pp. 100-112 (In Russian).

DOI: https://doi.org/10.33051/2500-2325-2020-4-100-112