DOI 10.37882/2223–2974.2022.05.26

# ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИИ В СОВРЕМЕННЫХ УСЛОВИЯХ

## FEATURES OF ENSURING INFORMATION SECURITY OF RUSSIA IN MODERN CONDITIONS

***A. Pimenov***

*Summary.* The current stage of development of Russian society requires changes in the information sphere, which is the activity of information infrastructure, facilities that collect, form, distribute and use information, as well as the system of regulation of public relations. The author evaluates the legal mechanisms for ensuring information security in Russia, taking into account the aggravation of the information war against our country.

*Keywords:* information threats, information security.

***Пименов Александр Николаевич***
*Аспирант, Российский университет транспорта (Москва)*
*sannikolaich@inbox.ru*

*Аннотация.* Современный этап развития российского общества требует изменений в информационной сфере, представляющей собой деятельность информационной инфраструктуры, объектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования общественных отношений. Автор оценивает правовые механизмы обеспечения информационной безопасности в России с учетом обострения информационной войны против нашей страны.

*Ключевые слова:* информационные угрозы, информационная безопасность.

Информационная сфера сегодня быстро и активно влияет на состояние политической, экономической безопасности Российской Федерации, а также непосредственно ее обороноспособность. Национальная безопасность Российской Федерации во многом зависит от обеспечения информационной безопасности, и эта зависимость постоянно возрастает в процессе технического прогресса и развития общества.

Информационная безопасность Российской Федерации выполняет защитную функцию национальных интересов страны в информационной сфере, сочетая баланс личности, общества и государства [3, с.57]. Сегодня задача обеспечения информационной безопасности, в том числе в сетях Интернета, является одной из форм защиты от так называемых «новых форм агрессии» в отношении Российской Федерации. Эти факторы обуславливают актуальность нашего исследования.

Информационная безопасность является одним из стратегических направлений в нынешней военно-политической ситуации. Работа в этом направлении ведется в рамках обеспечения вооруженных сил современными технологиями и направлена на создание военного превосходства России над потенциальными агрессорами. Следует отметить, что информационная безопасность способствует повышению качества стратегических ядерных сил, развитию боевых возможностей армии и флота и является основой для развития нового вида вооруженных сил — военно-космических сил. Информационная агрессия используется вместе с политическим и экономическим давлением.

В условиях существующей информационной войны российское правительство должно быть готово к любым, даже самым неожиданным, санкционным решениям со стороны «непредсказуемых» США и ЕС. Западные страны уже задумались об отключении россиян от Интернета из-за «постоянных хакерских атак с российской стороны» [7]. Хотя Россия ничего подобного не делала. Представители НАТО неоднократно заявляли о попытках взлома их веб-сайтов и кражи информации специального назначения с российских доменов. ИТ-специалисты очень хорошо понимают, кто является главным администратором глобальной сети Интернет. В связи с тем, что предсказать поведение западных «партнеров» (в нынешних условиях данное понятие перестает быть актуальным) практически невозможно, и нет оснований ожидать чего-либо хорошего, мы должны быть готовы к тому, что Россию исключат из глобального информационного/IT пространства.

Таким образом, возможность создания автономной сети «Рунет» можно считать одним из шагов в области обеспечения национальной информационной безопасности. Уже ни для кого не секрет, что у российских операторов есть механизм отключения России от Интернета

в случае чрезвычайной ситуации. Если вспомнить беспорядки в Египте в 2011 году, то местные власти отключили интернет и мобильные сети по всей стране. Теперь российские специалисты из Федерального агентства связи могут не только отключать Интернет, но и администрировать домены на собственной территории.

Министерство цифрового развития, связи и массовых коммуникаций РФ уже способно обеспечить автономную работу Рунета, не подключаясь к глобальному Интернету.

По данным аналитического агентства Positive Technologies, по словам заместителя генерального директора по развитию бизнеса Бориса Симиса, в 2021 году запланированные бюджеты на информационную безопасность увеличились в среднем на 20%, т.е. рынок вырос. Однако это формальный рост: если оценивать его в пересчете на фактически потраченные и заработанные участниками рынка деньги, то общая планка практически не превышает показателей 2020 года. Причина невыполнения бюджетов в большинстве случаев заключается в необходимости проходить конкурсные процедуры: компании просто не успевают закупать те средства защиты, которые запланированы или необходимы для сохранения информации и защиты от хакерских атак.

В последние пару лет уже было отмечено, что обеспечение информационной безопасности начало меняться и все больше компаний приходят к пониманию того, что необходимо построить такую систему защиты, которую невозможно взломать, но сегодня это очень сложно, учитывая развитие искусственного интеллекта и технологический прогресс. Значительная часть систем либо уже скомпрометирована, либо может быть скомпрометирована, и основная цель любой системы безопасности — как можно быстрее обнаружить злоумышленника и сократить для него возможность нанести непоправимый вред. В связи с этим наблюдается рост спроса на высокоинтеллектуальные средства защиты, позволяющие решать задачи по своевременному выявлению атак и инцидентов. В частности, речь идет о системах информационной безопасности класса и управления событиями (SIEM), анализа сетевого трафика (NTA), комплексных противоаварийных решениях.

Компании, которые стремятся действительно защитить себя в киберпространстве, сегодня сталкиваются с полной нехваткой персонала. Существует нехватка специалистов, обладающих достаточным уровнем компетентности, чтобы обеспечить высокий уровень способности к обнаружению (т.е. глубоко погруженных в специфику бизнеса защищаемых компаний, следящих за тенденциями безопасности и атак, понимающих новейшие технологии и их уязвимости). Мы видим, что растет спрос на специалистов сразу с несколькими компетенциями: это может быть сочетание знаний в области науки о данных и кибербезопасности, глубокой отраслевой специфики (скажем, автоматизированных систем управления) и информационной безопасности и т.д. Бизнес в результате осознает, что у него нет необходимого количества специалистов такого уровня, и обычно приходит на аутсорсинг или аутстаффинг, а в редких случаях даже вынужден самостоятельно обучать персонал, которого не хватает на рынке. Задачи информационной безопасности все чаще находят отражение в инициативах регулирующих органов: последние требования, стандарты и нормативные акты Центрального банка, Федеральной службы безопасности (ФСБ), Федеральной службы по техническому и экспортному контролю (ФСТЭК) направлены именно на практическое обеспечение безопасности в информационной сфере.

В частности, в 2019 году произошли ключевые изменения в законодательстве о защите объектов критической информационной инфраструктуры (КИИ), а также в нормативных актах Центрального банка и Федеральной службы безопасности. Наиболее важными в сфере КИИ являются новые методические документы, определяющие порядок взаимодействия между подразделениями критической информационной инфраструктуры и Национальным координационным центром по компьютерным инцидентам. В них объясняется, о каких происшествиях сообщать, какую информацию передавать, в какой срок. Начала функционировать «концепция» глобальной системы сбора и обмена информацией о компьютерных атаках в России, сформулированная в приказах ФСБ № 196, 281, 282 [3; 4; 5]. В них описываются инструменты, которые будут использоваться центром ГосСОПКА.

Кроме того, начала развиваться практика привлечения к ответственности по статье 274 Уголовного кодекса («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»), но пока только в отношении очевидных вещей: наказывают за нападения на объекты КИИ и за серьезные нарушения должностных инструкций.

В 2022 году предполагается внесение поправок в Федеральный закон от 26 июля 2017 г. N187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», будут исправлены неоднозначные термины и формулировки.

Также разрабатываются методические документы ФСТЭК по анализу угроз в информационных системах.

Вступили в силу три положения о платежных услугах Центрального банка. Основной вывод — с 1 января

2020 года финансовые организации должны использовать программное обеспечение, имеющее либо сертификат ФСТЭК, либо сертификат анализа уязвимостей. Мы не ожидаем, что разработчики банковского программного обеспечения начнут проводить массовую сертификацию своих решений, поскольку из всех сертификационных тестов фактически требуется только анализ уязвимостей и незадекларированных возможностей. Это традиционная услуга, востребованная кредитными организациями с высоким уровнем зрелости, но теперь она становится обязательной для всех финансовых организаций. Следует отдельно отметить, что процедура анализа уязвимостей, на которую ссылается регламент Центрального банка, требует, чтобы разработчики программного обеспечения проводили такой анализ самостоятельно, в рамках жизненного цикла разработки своих продуктов.

Уже сегодня это всколыхнуло рынок банковских услуг, и потребители банковского программного обеспечения начали заказывать услуги анализа безопасности. Для самописного программного обеспечения банки активно заказывают статический и динамический анализ кода. Если раньше такие услуги представляли интерес в основном для энтузиастов из финансовых компаний, то сейчас в них нуждаются все без исключения финансовые организации. Анализ безопасности стоит довольно дорого, исполнителей мало, и вам приходится конкурировать за них уже сейчас. В последнее время спрос вырос настолько резко, что предложение не успевает. Эксперты крупнейших компаний в сфере обеспечения информационной безопасности (их на российском рынке четыре или пять) могут провести 30–50 анализов безопасности в год, а у каждого банка из первой десятки таких приложений может быть 15–20. И эти приложения регулярно обновляются, что требует дополнительных проверок на уязвимости. Если организация имеет много приложений и часто выпускает обновления, будет выгоднее построить безопасный процесс разработки. Для поставщиков финансового программного обеспечения прохождение анализа уязвимостей становится конкурентным преимуществом. Уже сейчас многие разработчики банковского программного обеспечения говорят о подписании контрактов с ведущими компаниями в сфере информационной безопасности на работу по анализу исходного кода.

Мы ожидаем, что в ближайшие два-три года построение проверенного цикла безопасной разработки станет основным направлением для поставщиков банковского программного обеспечения. Чтобы устранить неопределенность и расплывчатость в требованиях к анализу безопасности, технический комитет Центрального банка (ТК № 122) разработал проект методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций», где подробно написано, как необходимо проводить анализ уязвимостей приложений.

Для России это первый опыт обязательного нормативного документа, такое уточнение было только в системе сертификации. Профиль защиты является обязательным документом, он предназначен для открытого рынка, и необходимо соответствовать этому документу. Не исключено, что примеру Центрального банка последуют и другие ведомства.

Следует также отметить появление закона о «суверенном Интернете» [2]: это первый случай, когда федеральный закон обязывает коммерческие компании (в данном случае — операторов связи) проводить киберучения. Ранее никто не обязывал компании оценивать в такой форме, насколько система способна противостоять злоумышленникам. Аналогичные требования к владельцам значимых объектов КИИ появились в требованиях ФСБ (владельцы значимых объектов КИИ обязаны составлять планы реагирования на инциденты и отрабатывать их во время учений).

В то время как тренинги по противодействию киберпреступности ранее проводились в организациях с высоким уровнем зрелости, в ближайшие два-три года они будут проводиться во многих компаниях: эти требования распространяются на всех операторов КИИ.

Анализируя вышесказанное, можно сделать вывод, что усложнение информационного взаимодействия между людьми, автоматизация управления промышленными объектами, транспортом и энергетикой создали новые возможности для целенаправленного негативного воздействия, которое может осуществляться как недружественными государствами, отдельными группами преступной направленности, так и отдельными лицами. Реализацию такой возможности обычно называют информационным терроризмом. Один квалифицированный хакер способен нанести ущерб, сравнимый с боевой операцией, проводимой воинской частью. В то же время территориальное расположение государств, создающее естественные препятствия для проведения традиционных операций, не является преимуществом при информационных атаках. Разработка информационного оружия не требует строительства заводов, его создание как государствами, так и отдельными лицами пока не может эффективно контролироваться.

Следовательно, необходимо создать правовую и организационную систему, способную координировать развитие информационной инфраструктуры нашей страны с целью предотвращения или максимальной

локализации последствий информационной войны или отдельных эпизодов применения информационного оружия. Это должно быть сделано без промедления. В соответствии со статьей 20 Закона об информации [1] основными задачами в области защиты информации являются: во-первых, защита граждан России от кражи и потери личной информации; во-вторых, для создания действий по предотвращению угроз безопасности граждан, общества и государства; в-третьих, для предотвращения несанкционированных действий по изменению, искажению, копированию или блокированию информации; в-четвертых, блокирование других форм незаконного вмешательства в информационные ресурсы и информационные системы; в-пятых, контроль за соблюдением конституционных прав граждан на сохранение личной тайны и защиту персональных данных, доступных в информационных системах; сохранение государственной тайны, конфиденциальность документированной информации в соответствии с законодательством.

Накопление проблем информационной безопасности в различных областях достигает своего предела. Аппаратные уязвимости еще не нанесли ущерба, но дальновидные компании начали включать такие проблемы в свою модель угроз уже сейчас, понимая, что когда преступники научатся использовать такие уязвимости, будет слишком поздно защищать себя.

Новости об утечках данных стали особенно громкими еще и потому, что киберпреступники предположительно объединили утечки прошлых лет в единый массив для торговли на теневом рынке с более полными цифровыми пользовательскими данными. У многих технологий есть своя темная сторона, которая может выйти из-под контроля и стать угрозой для всех. С предстоящим распространением сетей 5G эксперты связывают появление новых рисков для операторов связи. Развитие технологий искусственного интеллекта и машинного обучения не только делает жизнь более удобной, но и дает мощный толчок для совершенствования хакерских инструментов, а также новых методов социальной инженерии. Комплексная интеграция технологий порождает множество векторов атак. Противодействие угрозам в постоянно меняющемся мире современных технологий и адаптация к новым потребностям корпоративных и частных пользователей являются главными приоритетами для специалистов по информационной безопасности, решение которых может потребовать принципиально новых подходов к обеспечению кибербезопасности.

ЛИТЕРАТУРА


1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N149-ФЗ.
2. Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»».
3. Приказ ФСБ России от 6 мая 2019 г. N196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».
4. Приказ ФСБ России от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» (не вступил в силу).
5. Приказ ФСБ России от 19 июня 2019 г. N282 «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».
6. Чеботарева А.А. Теоретико-методологические подходы к правовому обеспечению информационной безопасности личности // Право и государство: теория и практика.— 2017.— 6 (150).— С. 149–152.
7. Чеботарева А.А., Ермошина Р.А. Взаимодействие законодательной, исполнительной и судебной власти в реализации информационной функции государства // Российская юстиция, (12):56–60, 2010.
8. Bamberger Kenneth A. and Mulligan Deirdre K. (2015) Privacy on the Ground: Driving Corporate Behavior in the United States and Europe. Cambridge, Massachusetts: MIT Press. P. 45–47.
9. Crawford Kate (2016) Artificial Intelligence's White Guy Problem // The New York Times, June 25.
10. Ferrucci David A. (2012) Introduction to «This is Watson» // IBM Journal of Research and Development. 2012. Issue 3. P. 235–249.
11. Ilyin I.V., Rozanov A.S. (2013) The impact of globalization on the formation of a global political system // Campus-Wide Information Systems.— Emerald Group Publishing Limited.— DOI: 10.1108/CWIS-08–2013–0037
12. Paz C.A. (2021) Legal Challenges for Artificial Intelligence in Chile // Revista Chilena de Derecho y Tecnologia.




Журнал «Современная наука: актуальные проблемы теории и практики»