Глушко Максим Сергеевич,
студент, ФВУНЦ ВВС «ВВА»
РФ, г. Челябинск

Еврасов Александр Евгеньевич,
студент, ФВУНЦ ВВС «ВВА»
РФ, г. Челябинск

Попов Юрий Леонидович,
кандидат исторических наук, доцент,
ФВУНЦ ВВС «ВВА», РФ, г. Челябинск

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ИНОСТРАННЫХ ГОСУДАРСТВ

Аннотация: В статье рассматриваются основные подходы к обеспечению информационной безопасности в ряде ведущих стран мира – Соединённых Штатов Америки, Китайской Народной Республики и Федеративной Республики Германия. Изучаются законодательные основы, ключевые государственные органы и практики защиты данных в каждой из них. Приводится сравнительный анализ отдельных элементов систем информационной безопасности иностранных государств с существующей российской системой. Результаты показывают различия в приоритетах, а также акцент российского законодательства на государственном контроле и полномочиях спецслужб.

Ключевые слова: информационная безопасность, кибербезопасность, защита персональных данных, законодательство, США, Китай, Германия, Россия.

1. Введение

Информационная безопасность является ключевым фактором национальной безопасности практически всех развитых стран мира. В условиях непрерывной цифровизации государства усиленно развивают законодательную базу и институты для защиты своих информационных систем, персональных данных и критической инфраструктуры. В этой статье анализируются подходы к защите информации в США, Китае и Германии, рассматриваются соответствующие нормативно-правовые акты, ключевые регулирующие органы и практики обеспечения безопасности данных. Также проводится сравнительный анализ этих подходов с российской системой информационной безопасности.

2. Система информационной безопасности США

В США вопросы кибербезопасности и защиты информации решаются преимущественно в контексте защиты критической инфраструктуры и права частной собственности. Федеральное правительство выстраивает системы, а крупные компании и правительства активно сотрудничают по принципу «частно-государственного партнёрства». Ключевое агентство – CISA (Cybersecurity and Infrastructure Security Agency), созданное в составе Министерства внутренней безопасности (DHS) и отвечающее за защиту критических государственных систем и инфраструктуры. Кроме того, Национальное агентство безопасности США (NSA) занимается обеспечением защиты национальных военных и правительственных сетей, а ФБР – расследованием киберпреступлений и атаками на сети (под «киберпреступлением» понимаются взломы, распространение вредоносного ПО и т.д. В сфере законодательства в США отсутствует единый всеобъемлющий закон о защите персональных данных: вместо этого действуют многочисленные отраслевые и региональные нормы (закон HIPAA по защите медицинских данных, закон GLBA о финансовой информации,

калифорнийский CCPA и др.), а также фед. законы об информационной безопасности федеральных систем (например, FISMA 2002). Такая «клеёночная» модель означает, что защита данных носит фрагментарный характер, и унифицированный закон на национальном уровне отсутствует. В последние годы при администрации президента Байдена были изданы исполнительные указы (например, EO 14028 2021 г.) для ужесточения требований по кибербезопасности федеральных учреждений и операторов критической инфраструктуры. В целом политика США в области ИБ характеризуется акцентом на resilience (устойчивость систем), координацию с частным сектором и активное развитие угрозной разведки (к примеру, Центр аналитики киберугроз при DHS).

3. Система информационной безопасности Китая

В Китае информационная безопасность понимается шире, чем кибербезопасность: основное внимание уделяется контролю над национальным сегментом интернет-пространства и надзору за данными граждан. В центре нормативной системы стоит Закон КНР о кибербезопасности (принят 2016 г., вступил в силу в 2017 г.), который устанавливает правила для операторов сетей по сбору и хранению пользовательских данных, требования к инфраструктуре стратегических отраслей и провозглашает принцип «киберсуверенитета». После 2016 года приняты дополнительные законы: Закон о безопасности данных (2021) и Закон о защите персональных данных (PIPL, 2021), предусматривающий согласие субъектов данных, ограничения на передачу за границу и серьёзные штрафы за нарушения. Так, в Китае вводятся жёсткие требования по локализации данных: критически важные данные и персональная информация китайских граждан должны храниться на территории страны. Основными государственными институтами в сфере ИБ являются Центральное управление по делам киберпространства (CAC) – высший регулятор интернета и средств массовой информации, отвечающий за цензуру и политику в сети; Министерство промышленности и информационных технологий (MIIT) – контролирует безопасность телекоммуникаций; Министерство общественной безопасности (аналог МВД) – раскрытие и пресечение киберпреступлений; Министерство государственной безопасности – контрразведка. Подход Китая можно охарактеризовать как «жёсткий контроль сверху»: крупные технологические компании обязаны проходить государственную сертификацию безопасности, а иностранные продукты (например, телеком-оборудование) подлежат особому надзору. На практике Китай известен «Великим файрволом» – системой цензуры и фильтрации контента, а также широким использованием цифрового мониторинга. Развитая законодательная база фиксирует принцип «первой политики по безопасности» над инновациями: приоритет – обеспечение партийного контроля и обороноспособности сети.

4. Система информационной безопасности Германии (ЕС)

ФРГ действует в рамках европейских стандартов кибербезопасности и защиты данных, в частности исполнение Регламента ЕС 2016/679 (GDPR) обобщает европейский подход. Федеральный закон Германии о защите данных (Bundesdatenschutzgesetz, BDSG) гармонизирован с GDPR (вступил в силу 25 мая 2018 г.) и использует «открытые» положения регламента. В результате в Германии действуют строгие требования к прозрачности обработки ПДн, широкой ответственности контролёров данных и высоким штрафам за нарушения. В части кибербезопасности центральным органом является Федеральное ведомство по безопасности информационных технологий (BSI). BSI разработан ещё в 1991 г. и отвечает за сертификацию ИТ-продуктов, безопасность правительственных систем, защита критических инфраструктур и контроль технологических стандартов. Законы об ИТ-безопасности укрепляются: так, IT-Sicherheitsgesetz (IT-SiG) 2015 и обновлённый IT-SiG 2.0 (2021) расширили полномочия BSI по выявлению уязвимостей, надзору за операторами связи (включая запрет использования небезопасных компонентов, например, при 5G) и созданию

национальной системы реагирования на инциденты. Кроме того, в Германии работают ФБР-подобный Федеральный офис по защите конституции (BfV), который занимается разведывательными задачами по киберугрозам, и Федеральный комиссар по защите данных (BfDI) – надзор за соблюдением норм о ПДн. В целом можно сказать, что германская модель ориентируется на превентивную защиту критической инфраструктуры и личной информации, с активным применением стандартов и сертификаций. С одной стороны, это гарантирует высокий уровень защиты данных, с другой – существенные расходы и бюрократию для бизнеса.

5. Система информационной безопасности России

Российская модель информационной безопасности сочетает в себе элементы контроля над информационным пространством и защиты критической инфраструктуры. Ключевые документы – Концепция национальной безопасности РФ (2015, обновлённая в 2021), Концепция информационной безопасности РФ (2016) и «Стратегия национальной безопасности», где одним из приоритетов названо «обеспечение информационного суверенитета» страны. В законодательстве закреплены многочисленные нормы: например, Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» (2006) устанавливает общие принципы, ФЗ-152 «О персональных данных» (2006, с поправками) регламентирует обработку личной информации, ФЗ-187 «О безопасности критической информационной инфраструктуры» (2017) вводит особые требования для объектов КИИ, а антитеррористические законы («пакет Яровой» 2016) обязали операторов связи хранить метаданные. Основные органы – ФСБ (контролирует использование криптографии, ведёт тайный надзор за информацией), ФСТЭК России (ведомство под Минцифры – ставит требования по технической защите информации, сертификация средств защиты, контроль безопасности государственных систем), Роскомнадзор (регулятор связи и СМИ – надзор за соблюдением закона о ПДн и за контентом в интернете), а также МВД (центр по борьбе с киберпреступностью) и специальные подразделения (например, ЦНИИС ФСБ, Центр мониторинга киберугроз). Практики защиты данных включают строгие требования по локализации персональной информации («данные российских граждан должны храниться в России»), обязательную регистрацию операторов связи и мессенджеров (мессенджеры обязаны предоставлять ключи шифрования по запросу ФСБ). В отличие от США и ЕС, в России нет акцента на общественное доверие и баланс с приватностью; напротив, государственный контроль и безопасность по определению стоят выше свободы информации.

6. Сравнительный анализ и таблицы

Приведём основные различия в подходах четырёх стран в табличной форме. В таблице 1 показаны ключевые законодательные акты и институциональные особенности. Таблица 2 содержит сведения о главных государственных органах и их функциях в области ИБ. Такие сравнения наглядно демонстрируют, что в США и Германии (ЕС) информационная безопасность делается акцентом на защиту частных данных и критических систем в рамках законодательной рамки, в то время как Китай и Россия больше ориентированы на национальный контроль (табл. 1–2). Например, в Китае вводится уголовная ответственность за «нарушение национального киберсуверенитета», а в ЕС – тяжёлые штрафы за утечки персональной информации. В США же, несмотря на большое число инцидентов, отсутствует единое понимание «личных данных» и централизованного надзора, что смягчает жестокость санкций, но усложняет единообразное регулирование. Российская система включает элементы всех подходов: с одной стороны, наличие закона о персональных данных (152-ФЗ) сближает её с западными нормами, а с другой – обширная силовая составляющая (ФСБ/ФСТЭК) делает её уникальной по уровню государственного вмешательства. Ниже в таблице 3 приведены некоторые примеры практических мер: они показывают, что, например, требования по шифрованию и доступу к данным в Китае и России куда строже, чем в Европе или США, где

упор делается скорее на стандарты и рекомендации. В целом можно заключить, что несмотря на общую цель – защиту информации – национальные стратегии заметно разнятся из-за политических и социальных факторов.

Таблица 1

Страна	Законодательство и политика	Ключевые органы	Особенности
США	FISMA, CISA Act (2018), секторные законы (HIPAA и др.), исполнительные указы (EO 2021) – нет единого закона о ПДн.	CISA (DHS); NSA; FBI	Секторный подход: защита инфраструктуры и правительственных систем; координация с частным сектором; фреймворки NIST.
Китай	Закон КНР о кибербезопасности (2016); Закон о безопасности данных (2021); PIPL – закон о ПДн (2021). Акцент на «киберсуверенитете».	Центральное управление по делам киберпространства (CAC); MIIT; МВД; МВД (MPS); МГБ (MSS)	Государственный контроль над интернетом и данными; обязательная локализация данных; цензура и мониторинг; строгие штрафы.
Германия (ЕС)	GDPR (2016); BDSG (2018) – национальный закон о защите данных; IT Security Acts 2015/2021 (увеличение полномочий BSI); директива NIS (дигитализация).	BSI (ведомство по ИБ); BfV (контрразведка); BfDI (комиссар по ПДн)	Строгая защита ПДн по европейским стандартам; BSI – главный орган по кибербезопасности; сертификация IT-продуктов.
Россия	ФЗ-149 «Об информации» (2006); ФЗ-152 «О персональных данных» (2006, обновлён 2021); ФЗ-187 «О КИИ» (2017); законы «пакета Яровой» (2016) и др. Принцип «информационного суверенитета».	ФСБ; ФСТЭК; Роскомнадзор; МВД (ЦБД)	Централизованная система с акцентом на гос. контроль: криптографические требования и запрет анонимных сервисов; обязательная локализация данных; жесткие санкции.

Таблица 2

Страна	Ключевые органы	Основные функции
США	**CISA (DHS); NSA; FBI**	Защита гос. и критических ИТ-систем; кибербразведка; расследование киберпреступлений.
Китай	**CAC**; **MIIT**; МВД (Public Security); МГБ	Регулирование и контроль интернета; противодействие киберугрозам; обеспечение «киберсуверенитета».
Германия	**BSI; BKA/BfV; BfDI**	Разработка стандартов ИБ; сертификация продуктов; борьба с киберпреступностью; надзор за ПДн.

Россия	**ФСБ; ФСТЭК; Роскомнадзор;** МВД	Криптографический контроль; защита информационных ресурсов государства; мониторинг и контроль ПДн.

7. Заключение

Между системами информационной безопасности разных стран наблюдаются существенные отличия, отражающие национальные приоритеты и политический строй. США делают упор на координацию с бизнесом и стандартизацию, но не имеют единого всеобщего закона о защите данных. Китай фокусируется на «киберсуверенитете» и жёстком контроле за контентом и данными. Германия (и ЕС) руководствуется философией защиты прав личности и безопасности инфраструктуры с помощью строгих регламентов (GDPR, BSI). Российская система характеризуется централизованным надзором и высоким уровнем государственного вмешательства. Сравнительный анализ показывает, что при явном общем стремлении к защите информации каждое государство выбирает свою модель – от демократически-ориентированных до авторитарных – в зависимости от политических и культурных факторов.

Список литературы:

1. Cybersecurity and Infrastructure Security Agency (CISA). Официальная информация DHS о CISA [Электронный ресурс]. – Режим доступа: https://www.cisa.gov.

2. Federal Bureau of Investigation (FBI). Cybercrime Overview [Электронный ресурс]. – Режим доступа: https://www.fbi.gov.

3. NSA/CSS Cybersecurity. Национальное агентство безопасности США: задачи по кибербезопасности [Электронный ресурс]. – Режим доступа: https://www.nsa.gov/cybersecurity.

4. DLA Piper. Data protection laws in the United States [Электронный ресурс]. – Режим доступа: https://www.dlapiperdataprotection.com.

5. Закон КНР о кибербезопасности от 07.11.2016. – Сборник законодательства КНР.

6. The Personal Information Protection Law of the People’s Republic of China (PIPL) от 20.08.2021 [Электронный ресурс]. – Режим доступа: https://personalinformationprotectionlaw.com.

7. Bundesamt für Sicherheit in der Informationstechnik (BSI). Информация о Законе об ИТ-безопасности 2.0 (Германия) [Электронный ресурс]. – Режим доступа: https://www.bsi.bund.de.

8. Bundesdatenschutzgesetz (BDSG) – Федеральный закон Германии о защите данных (2018).

9. Федеральный закон РФ от 27.07.2006 №152-ФЗ «О персональных данных». – КонсультантПлюс [Электронный ресурс]. – Режим доступа: https://www.consultant.ru.