

ОСНОВЫ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Я.С. Мелешенко, В.В. Васькевич

*Гомельский государственный университет имени Франциска Скорины,
Гомель, Беларусь*

Аннотация. В работе анализируются ключевые требования к обеспечению информационной безопасности в Республике Беларусь с приведением описания конкретных нормативно-правовых актов, регламентирующих вопросы обработки, хранения, передачи данных и вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов. Изложены основные факторы, способствующие совершению киберпреступлений и некоторые меры по защите информации, такие как правовые, организационные, технические, а также основные черты концепции информационной безопасности в стране. Описываются элементы национальной системы обеспечения кибербезопасности и акты, составленные в целях регулирования общественных отношений в данной сфере и обеспечения защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных. Рассматриваются общие принципы реализации и регулирования защиты информации действующим законодательством.

Ключевые слова: информационная безопасность; закон; информационное общество; постановление; персональные данные; указ; национальная система; центр кибербезопасности; аттестация; защита информации.

FUNDAMENTALS OF NORMATIVE LEGAL REGULATION IN THE FIELD OF INFORMATION PROTECTION IN THE REPUBLIC OF BELARUS

Y. Meleshchenko, V. Vaskevich

Francisk Skorina Gomel State University, Gomel, Belarus

Annotation. The article analyzes the key requirements for ensuring information security in the Republic of Belarus with a description of specific normative legal acts regulating the processing, storage, transmission of data and issues of ensuring national security, including the security of the information space, information infrastructure, information systems and resources. The main factors contributing to the commission of cybercrimes and some information protection measures, such as legal, organizational, technical, as well as the main features of the information security concept in the country, are outlined. The article describes the elements of the national cybersecurity system and acts drawn up to regulate public relations in this area and ensure the protection of personal data, the rights and freedoms of individuals when processing their personal data. The general principles of implementation and regulation of information protection by the current legislation are considered.

Keywords: information security; law; information society; resolution; personal data; decree; national system; cybersecurity center; attestation; information protection.

Введение

В условиях становления общества особую ценность обретает информация, а вопросы ее безопасности становятся все более актуальными. В настоящее время сложно выделить сферу общественной деятельности, в которой бы не применялись информационные технологии. Однако с увеличением доли населения, использующей информационные технологии, происходит увеличение количества преступлений в сфере ИТ. Совершению подобных преступлений способствуют компьютерная неграмотность сотрудников, отсутствие механизмов контроля и проверки поступающей электронной информации или недостаточность их реализации. Количество киберпреступлений в Беларуси в 2024 году составило более четверти от всех преступлений в стране [1].

В Республике Беларусь существует ряд требований законодательства, осуществляющих защиту информации. Защита информации - комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Основная часть

Основой нормативно-правового регулирования в рассматриваемой сфере является Закон РБ 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», которым регулируются общественные отношения, возникающие при:

- поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также использовании информацией;
- создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;
- организации и обеспечении защиты информации.

В Законе определены некоторые меры по защите информации, такие как правовые, организационные, технические. К правовым мерам по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также

ответственность сторон по договору за нарушение указанных условий. К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации. К техническим мерам по защите информации относятся меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации.

18 марта 2019 г. Президентом было подписано постановление Совета Безопасности Республики Беларусь №1 «О Концепции информационной безопасности Республики Беларусь». В нем отмечено кардинальное повышение роли информационных технологий в реализации прав и свобод граждан, а также сопутствующие трансформации социума в информационное общество порождение новых рисков, вызовов и угроз, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов. Формирование в Республике Беларусь информационного общества, обеспечивающего доступность информации, распространение и использование знаний для поступательного и прогрессивного развития, рассматривается как национальный приоритет и общегосударственная задача. Концепция представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности [2].

В рамках Закона РБ от 7 мая 2021 г. №99-З «О защите персональных данных» в целях обеспечения защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных было постановлено создать Национальный центр защиты персональных данных Республики Беларусь.

С целью обеспечения безопасности национальной информационной инфраструктуры в Республике Беларусь 14 февраля 2023 года был подписан Указ Президента Республики Беларусь №40 «О кибербезопасности». В котором было постановлено о необходимости создать в Республике Беларусь национальную систему обеспечения кибербезопасности, элементами которой являются:

- Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ);
- Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты (далее – Национальный центр кибербезопасности);
- Центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности);
- Оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций (далее – авторизованный оператор электросвязи);
- Объекты информационной инфраструктуры государственных органов и иных организаций (далее – объекты информационной инфраструктуры);
- Сети передачи данных, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности, указанных в абзацах втором-пятом настоящего пункта [2].

Кроме того, указом определены основные задачи национальной системы обеспечения кибербезопасности.

Компании всех размеров сталкиваются с необходимостью защиты информации, так как кибератаки могут иметь серьезные последствия, включая финансовые потери, вред репутации, утрату доверия со стороны клиентов и нарушение сохранности интеллектуальной собственности, поэтому внедрение надежной системы кибербезопасности является не только соблюдением нормативных требований, но и стратегически важным решением.

25 июля 2023 вышел Приказ Оперативно-аналитического центра при президенте Республики Беларусь № 130 «О мерах по реализации Указа президента Республики Беларусь от 14 февраля 2023 г. № 40». В нем подробно описаны условия, необходимые для обеспечения информационной безопасности, формализованы алгоритмы действий при возникновении киберинцидентов, также описана типовая структура центров кибербезопасности и требования к ним.

В настоящее время в Республике Беларусь созданы Оперативно-аналитический центр при Президенте Республики Беларусь и центры по кибербезопасности, 17 из которых прошли проверку ОАЦ. Их задача – предотвращение и минимизация последствий атак на объекты информационной инфраструктуры. Аттестация SOC (Security Operations Center) в Беларуси предусматривает проверку соответствия программных и аппаратных средств определенным требованиям, систем защиты информации и компетенций персонала. Центр кибербезопасности Республиканского унитарного предприятия «Национальный центр обмена трафиком» по приказу от 11.11.2023 №204 стал первым в Республике Беларусь аттестованным центром кибербезопасности. Таким образом в стране было положено начало официальной деятельности по защите информации. Первой в стране коммерческой организацией, получившей такую аттестацию, стало Общество с ограниченной ответственностью «Надежные программы» (приказ от 05.01.2024 №1) [3].

С развитием сферы кибербезопасности растет спрос на высококвалифицированных работников в этой сфере. Для подготовки специалистов в Республике Беларусь осуществляется набор на специальность «Кибербезопасность» в следующих вузах: Гомельский государственный университет имени Франциска Скорины, Гродненский государственный университет имени Янки Купалы, Белорусский государственный университет, Полоцкий государственный университет имени Евфросинии Полоцкой. Подготовка специалиста по данной специальности предполагает формирование определенных профессиональных компетенций, включающих знания и умения в области разработки и эксплуатации средств и систем защиты информации, осуществления контроля за их использованием. Специалист по кибербезопасности должен уметь защищать информационные системы от взломов, выявлять угрозы информационной безопасности и риски потери данных, обеспечивать сохранность и конфиденциальность данных.

Заключение

В современном мире информация – ценный продукт. Поэтому услуги по защите информации характеризуются высоким спросом и их актуальность подтверждается на законодательном уровне. Благодаря четко регламентированной политике организаций по обеспечению защиты информации осуществляется построение национальной системы кибербезопасности.

Список использованных источников

1. Иванова. Д. Каждое четвертое преступление в Беларуси совершили кибермошенники. В ГУВД привели статистику 2024 года. [Электронный ресурс] / Д. Иванова // Минск новости: публикация. – 2024. – 13 ноября. – URL: <https://minsknews.by/v-2024-godu-kiberprestupleniya-v-belarusi-sostavili-chetvert-ot-vsch-pravonarushenij/>. – Дата доступа: 25.02.2025.

2. О концепции информационной безопасности Республики Беларусь: Постановление совета безопасности республики Беларусь от 18 марта 2019 г. №1 [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – 2019. – 20 марта. – URL: <https://pravo.by/document/?guid=3871&pr0=P219s0001/>. – Дата доступа: 25.02.2025.

3. Перечень аттестованных центров кибербезопасности [Электронный ресурс] // Оперативно-аналитический центр при Президенте Республики Беларусь. – Режим доступа: www.oac.gov.by/activity/cybersecurity-centers-list/certified-cybersecurity-centers/ – Дата доступа: 25.02.2025.

Сведения об авторах

Мелещенко Я.С., студентка 2 курса факультета физики и информационных технологий специальности «Кибербезопасность». Гомельский государственный университет имени Франциска Скорины. na.ya.mo@mail.ru.
Васкевич В.В., старший преподаватель кафедры радиофизики и электроники. Гомельский государственный университет имени Франциска Скорины. vaskevich@gsu.by.

Information about the authors

Meleshchenko Y., 2nd year student of the Faculty of Physics and Information Technology specialty "Cybersecurity". Francysk Skaryna Gomel State University. na.ya.mo@mail.ru.
Vaskevich V., Senior Lecturer at the Department of Radiophysics and Electronics. Francysk Skaryna Gomel State University. vaskevich@gsu.by.