УДК 004.056.5
https://doi.org/10.36906/KSP-2021/17

Морозков В.А.
ORCID: 0000-0003-3989-8121, канд. юрид. наук
Афонина К.А.
ORCID: 0000-0002-2078-4645
Сургутский государственный университет
г. Сургут, Россия

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

Аннотация. В статье рассматриваются вопросы обеспечения информационной безопасности субъектов экономических отношений, содержания её основных элементов и средств защиты информационных ресурсов. На основе данных сформулированы рекомендации по разработке и внедрению эффективной политики информационной безопасности, действующей на предприятии.

Ключевые слова: экономическая безопасность; защита данных; политика информационной безопасности.

Morozkov V.A.
ORCID: 0000-0003-3989-8121, Ph.D.
Afonina K.A.
ORCID: 0000-0002-2078-4645
Surgut State University
Surgut, Russia

INFORMATION SECURITY POLICY IN THE CONTEXT OF ENSURING THE ECONOMIC SECURITY OF THE ECONOMIC ENTITY

Abstract. This article discusses the issues of ensuring information security of subjects of economic relations, the content of its main elements and means of protecting information resources. Based on the data, recommendations were formulated for the development and implementation of an effective information security policy in force at the enterprise.

Key words: economic security; data protection; information security policy.

Отличительным признаком современности является переход человечества к информационному сообществу. Цифра постепенно проникает во все сферы нашей жизни и оказывает на нас всё большее влияние.

Оцифровка на сегодняшний день приводит к исчезновению многих секторов экономики, наряду с предприятиями и рабочими местами, меняет социальное поведение людей, воздействует на трудовые отношения и на отношения собственности. В результате чего страны теряют право получать прибыль от этой стоимости, созданной на их территории. В этой связи роль государства и организации работы федеральных и иных органов власти должна быть переосмыслена относительно цифровой модификации (https://ria.ru).

Основополагающим нормативным правовым актом, способным урегулировать правоотношения в сфере цифровых технологий на основе формирования эффективной системы обеспечения информационной безопасности является Федеральный закон от 27.07.2006 № 149 «Об информации, информационных технологиях и защите информации».

Однако, как показывают материалы следственно-судебной практики, за семь месяцев 2021 года произошло почти 320 000 киберпреступлений, что на 16% больше, чем за аналогичный период прошлого года. Многочисленные исследования показывают, что определяющее влияние оказывают киберпреступники, чаще всего атакующие внешние ресурсы: клиентские порталы (40%), сервисы связи (36%) и сайты (52%). Вместе с тем следует подчеркнуть, что 82% угроз совершается служебным персоналом и самими пользователями компьютеров в случае их прямого или косвенного участия (https://clck.ru/UY4zY).

Поскольку информация для производителя является ценной, так зачастую её создание и приобретение весьма трудоемкий и дорогостоящий процесс, соответственно вышеприведенная статистика позволяет увидеть глубину и степень опасности рассматриваемой проблематики. Последствия от несанкционированного доступа к информационным ресурсам являются большими препятствиями в механизме их обработки и передаче как пользователям, так и субъектам управления в данной сфере, включая финансовую, коммерческую и другие составляющие конфиденциальной информации. В этой связи качество обеспечения функции информационной составляющей экономической безопасности хозяйствующего субъекта является весьма проблематичной [3, с. 5].

Экономическая и информационная интернационализация международных отношений сопровождается созданием эффективных систем и средств для информационно-финансового воздействия на деловое пространство. Данная система может обеспечивать как защиту конкретного узла индивидуально, так и целого сетевого сегмента.

Защита корпоративной информационной среды традиционно содержит: мониторинг материалов сбор информации об эвентуальных устроителей промышленного шпионажа и осуществление соответствующих превентивных мероприятий с целью выявления, локализации и пресечения возникающих фактов угрозы; перекрытие несанкционированного доступа к производственным помещениям, транспорту, материальным и цифровым носителям информации в рамках реализации административно правого режима защиты охраны объекта.

В рамках экономической безопасности организации информационная безопасность включает в себя: комплексную программу обеспечения безопасности информационных ресурсов предприятия; экономически обоснованную технологическую систему защиты

информационной безопасности, обеспечивающую должный уровень защищенности информационных систем.

В процессе обозреваемого вопроса следует отметить, что в Концепции и моделях менеджмента безопасности информационных и телекоммуникационных технологий, утвержденной государственным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Менеджмент безопасности информационных и телекоммуникационных технологий» (далее - Стандарт) указано, что основной целью введения системы информационной безопасности должно являться обеспечение устойчивого функционирования объекта, посредством предотвращения угроз его безопасности, защиты законных интересов клиента от неправомерного посягательства, предотвращения краж денежных средств и разглашений, утечек, искажения и уничтожения служебной информации, обеспечения стабильной деятельности всех подразделений хозяйствующего объекта. В п. 4 Стандарта определено, что наряду с целью, в качестве теоретической основы информационной безопасности следует рассматривать политику безопасности информационно-телекоммуникационных технологий (далее - ИТТ), поскольку совместно со стратегией, в своей совокупности, они определяют уровень безопасности для организации и порог приемлемого риска [1].

Не углубляясь в научную полемику в отношении соотношения указанных дефиниций, считаем необходимым акцентировать внимание на понятийном аппарате рассматриваемой категории. Под политикой информационной безопасности в специальной научной литературе в широком смысле принято понимать систему взглядов на проблему обеспечения информационной безопасности в автоматизированных системах (АС) общества. Соответственно, данная система взглядов содержит сгруппированное изложение целей и задач защиты, основополагающих начал и методов их реализации в достижении заявленного уровня информационной безопасности.

Рассматривая политику безопасности информационно-телекоммуникационных технологий хозяйствующего субъекта, в контексте Концепции, в качестве ее составляющих будут выступать правила, директивы, сложившаяся практика, определяющие степень критичности информации, а также механизм управления, защиты и предотвращения рисков и угроз. Отдельные исследователи полагают, что политика информационной безопасности должна содержать детали особых требований безопасности и защитных мер, подлежащих реализации, процедуры правильного использования защитных мер для обеспечения адекватной безопасности, устанавливать ответственность руководства [2]. Во всех случаях важно, чтобы реализуемая политика информационной безопасности была конструктивна и продуктивна в отношении интереса бизнеса компании.

Анализ практики по реализации политики информационной безопасности хозяйствующих субъектов позволяет сформулировать основные рекомендации по эффективному применению организационных аспектов в данной сфере:

– разработка четкой структуры управления для интеграции ИТТ в производственный механизм и обеспечение постоянного контроля информационной безопасности в организации;

– пересмотр локальных нормативных правовых актов, в том числе должностных регламентов персонала в отношении оптимизации элементов административной правосубъектности в рамках трудовых правоотношений;

– поддержание на соответствующем уровне безопасности режима конфиденциальности служебной информации, с разработкой и принятием соответствующего пакета локальных нормативных правовых актов и созданием условий для его обеспечения.

– разработка и реализация механизма взаимодействия с внешними инстанциями, например, подрядчиками, энергоснабжающей компанией, и с отдельными специалистами.

В качестве основных выводов отметим следующие:

1. Направления развития политики безопасности должны формироваться на основании апробированной модели угроз безопасности информации, разработанной статистическим методом, картой рисков, методом аналогий и методом экспертных оценок, в которой идентифицированы актуальные угрозы и их источники, нарушители посредством оценки возможности реализации угрозы и степени нанесения ущерба от них. Процесс управления рисками протекает путем систематического применения политик, процедур, практик мониторинга и анализа хозяйствующей деятельности субъекта;

2. Политика безопасности охватывает практически все аспекты деятельности организации, так или иначе связанные с обработкой, хранением, передачей информации. Поэтому необходима детальная разработка и внедрение данного документа в целях защиты информации от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи и обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности предприятия;

3. На сегодняшний день при разработке политики безопасности стоит учитывать появление новых угроз, технологий и бизнес-моделей, из которых наиболее перспективными направлениями являются: «интернет поведения» (IoB), пограничные сервисы безопасного доступа (SASE), моделирование взлома и атаки (BAS), расширенное обнаружение угроз и реагирование на них (XDR), идентификация сообщений, создание отчётов и определение соответствия по доменному имени (DMARC), анализа и предотвращения инцидентов (SIEM-системы), а также создание киберпространственного совета директоров и развитие киберграмотности среди населения (https://clck.ru/UY4zY);

4. Для реализации политики информационной безопасности организации, в силу включения информации во все элементы производственно-хозяйственной деятельности и понимании величины возможных потерь, ее полноценное обеспечение должно быть максимально регламентировано и постоянно контролироваться в полном объёме;

5. К обеспечению информационной безопасности необходимо применять многопрофильный подход. Это обусловлено тем, что информационная безопасность должна

обеспечиваться разными мерами и на нескольких уровнях, то есть представлять, как бы несколько эшелонов защиты информации. Как правило, политика безопасности рассматривается на трёх уровнях детализации, рассматривая политику безопасности как одну из организационных мер защиты информации, точнее, как одну из административных мер. На верхнем уровне принимаются решения, касающиеся организации в целом, в терминах целостности, доступности и конфиденциальности информации. На среднем уровне принимаются решения, касающиеся ответственности за соблюдение политики безопасности, обучения персонала, назначения ответственных лиц, и подобные вопросы. На нижнем уровне принимаются решения по конкретным системам и сервисам. Политика безопасности может быть, как самостоятельным документом, так и составлять часть документа по общей политике;

6. В реализации основных направлений политики безопасности информационно-телекоммуникационных технологий организации должны принимать участие представители направлений, связанных со всеми основными функциональными составляющими экономической безопасности субъекта финансово-хозяйственной деятельности, в том числе подразделениями и службами: внутреннего контроля, юридического сопровождения, финансово-экономической деятельности, информационной безопасности, коммунального хозяйства;

7. Особую роль следует уделять развитию кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

8. Немаловажное значение в обеспечении защищенности граждан от информационных угроз имеет создание и поддержание на предприятии механизма формирования культуры личной информационной безопасности;

9. Наиболее существенное влияние на состав и содержание разделов политики информационной безопасности организации оказывают международные и отечественные требования, действующие законодательства, но с высокой изменчивостью информационных технологий, технологий обеспечения информационной безопасности и появления новых средств информационной безопасности, а также с ростом возможностей нарушителя информационной безопасности, внутренние стандарты, политики и регламенты. Период актуализации частных политик информационной безопасности должен устанавливаться в один год;

10. Соблюдение правил и принципов безопасности производится основным инструментом контроля состояния защищенности информационной составляющей компании – аудитом, включая технический и организационно-методический аудиты. На этой стадии чаще всего аудит включает следующие направления: аудит ИТТ инфраструктуры и АС, контроль исходного кода приложений на уязвимости, тест на проникновение нарушителей (I.PEN-тест). Итоговым результатом процесса является составление заключения о степени соответствия хозяйствующего субъекта критериям аудита, указание рекомендаций по совершенствованию системы обеспечения и управления информационной безопасности, внесение корректирующих условий в политику безопасности организации;

11. Необходимо отметить, что существующая практики обеспечения экономической, физической, информационной безопасности хозяйствующих субъектов, в соответствии с Федеральным законом «О частной детективной и охранной деятельности в Российской Федерации», Федеральный закон «О ведомственной охране» и другими нормативными правовыми актами, данные функции исполняет значительное число участников правоотношений, способных обеспечить политику информационной безопасности от внутренних и внешних угроз, что позволяет уверенно осуществлять управление устойчивым развитием социально-экономической системы любого уровня.

Литература

1. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Ч. 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. М.: Стандартинформ, 2007.

2. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. М.: ИПК Издательство стандартов, 2002.

3. Мамаева Л.Н., Кондратьева О.А. Основные направления обеспечения информационной безопасности предприятия // Информационная безопасность регионов. 2016. №2. С. 5-9.