References

1. Antipenko, N. A. Ekonomika ustojchivogo razvitiya: kollektivnaya monografiya / N. A. Antipenko [i dr.] // Institut biznesa Bel. gos. universiteta. – Minsk : IVC Minfina, 2022. – 460 s.

2. Antipenko, N. A. Sistemnyj podhod k finansovomu analizu v ramkah koncepcii upravleniya cennost'yu / N. A. Antipenko, L. I. Tishchenko // Buhgalterskij uchet i analiz. – 2022. – № 7. – S. 50–54.

3. Antipenko, N. A. O metodike ocenki effektivnosti investicionnyh proektov / N. A. Antipenko // materialy H nauchnoj sessii prepodavatelej i studentov, 19, 20 apr. 2007 g. ; redkol.: I. V. Mandrik [i dr.]. – Vitebsk, UO FPB VM MITSO, 2007. – S.25–26.

4. Busygin, D. Yu. Analiticheskaya ocenka klyuchevyh metodov analiza ugrozy bankrotstva / D.Yu. Busygin // Buhgalterskij uchet i analiz. – 2023. – № 1. – S. 42–49.

5. Busygin, Yu. N. Osobennosti i puti sovershenstvovaniya dejstvuyushchej praktiki analiza kreditosposobnosti korporativnogo klienta bankom / Yu. N. Busygin, V. L. Savich // Fundamental'nye problemy ekonomiki : sb. statej Mezhdunar. nauch.-prakt. konf. 27, 28 sent. 2013 g.: v 2 ch. ; otv. red. R. G. YUsupov. – UFA: RIC BashGU, CH. 1 – 2013. – S. 21–23.

УДК 004

СОВЕРШЕНСТВОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

А. А. Евдокимова
Научный руководитель: Е. В. Зеленцова, к. т. н., доцент

Московский государственный технический университет имени Н. Э. Баумана
(национальный исследовательский университет)
Российская Федерация, г. Москва, ул 2-я Бауманская, д. 5, стр. 1
uaevdokimova@yandex.ru

В статье рассматриваются вопросы обеспечения информационной безопасности в Российской Федерации, сделан анализ существующих изменений в законодательном регулировании вопросов обеспечения информационной безопасности на национальном уровне, изучены технологические аспекты, выявлены основные тенденции изменений, подведены общие итоги.

Ключевые слова: информационная безопасность, законодательство, персональные данные, кибератаки, программное обеспечение.

IMPROVING INFORMATION SECURITY IN THE RUSSIAN FEDERATION

A. A. Evdokimova
Scientific supervisor: E. V. Zelentsova

Bauman Moscow State Technical University
(National Research University)
Russian Federation, Moscow, 2nd Baumanskaya str., 5, p. 1
uaevdokimova@yandex.ru

The article examines the issues of information security in the Russian Federation, analyzes the existing changes in the legislative regulation of information security issues at the national level,

examines technological aspects, identifies the main trends of changes, summarizes the overall results.

Keywords: information security, legislation, personal data, cyberattacks, software.

Возможности и риски цифровизации рождают необходимость постоянных изменений и трансформаций, требующих активного участия всех заинтересованных сторон [1]. В 2022 году в Российской Федерации проявилось множество непрогнозируемых факторов, оказавших активное влияние на развитие сектора информационной безопасности. Уход определенных западных компаний из страны и введение запретов на возможность использования определенного программного обеспечения привели к разрыву сформированных годами действующих логистических цепочек и необходимости активного формирования новых путей развития в данном секторе. На рынке возникла огромная потребность в альтернативных продуктах и технологиях.

Рассмотрим произошедшие на национальном уровне изменения и их влияние на информационную безопасность.

Законодательная база претерпела серьезные изменения. Начиная с 2025 года будет запрещено применение средств защиты информации, производители которых прямо или косвенно имеют отношение к странам, признанными Российской Федерацией недружественными. Предписано обязательное формирование структурных подразделений, предназначенных для обеспечения информационной безопасности стратегически важных организаций государственного и негосударственного сектора. Проведение анализа и оценки защищенности данных организаций возможно как на самостоятельной основе. так и с привлечением сторонних организации, обладающих полномочиями на проведение мероприятий по технической защите конфиденциальной информации [2].

Нововведения законодательного порядка коснулись также стандартов автоматизированных систем и информационной безопасности. С января 2023 года была обозначена необходимость наличия единой организации процесса идентификации субъектов и объектов доступа в средствах защиты информационного свойства, объектах вычислительной техники и применяемых в деятельности автоматизированных системах. Конкретизированы состав участников и основные параметры процесса идентификации, дано предписание по соблюдению определенного порядка первичной и вторичной идентификации, указаны правила и технологии управления доступом, рекомендуемые к применению в процессах разработки, введения в действие или оптимизации существующих механизмов. Стандарт также предусматривает возможность создания новых продуктов и решений автоматизированного свойства и новых отраслевых норм, детализирующих его предписания и не противоречащих ему [3].

Защита конфиденциальной информации активно выходит на первый план. Большинство кибератак в настоящее время направлено именно на персональные данные. Законодательство предписывает:

– проверку поручений на обработку персональных данных субъектов-носителей таких данных, конкретизируя требования ко всем обработчикам данных персонализированного свойства;

– отказ от избыточного сбора биометрии, так как субъекту – носителю персональных данных дали права на отказ в их предоставлении;

– проверку договоров с субъектами персональных данных, так как подобный договор не должен содержать позиции, рассматриваемые как ограничители прав и свобод субъекта персональных данных;

– проверку форм согласий на обработку персональных данных субъектов;

– проверку форм уведомлений субъектов – носителей персональных сведений;

– проверку регламента внутреннего аудита соответствия обработки персональных данных;

– публичное размещение (на сайте организации) политики в отношении обработки персональных данных.

– проверку регламента реагирования на инциденты, возникающие при выявлении фактов неправомерной или случайной передачи персональных сведений (24 часа дается на уведомление регулятора, 72 часа – на исправление возникшего инцидента);

– уведомление Роскомнадзора о трансграничной передаче персональных данных;

– разработку регламента уничтожения скомпрометированных в результате выявленного события персональных данных [4].

Выявлено увеличение кибератак и расширение зон их проникновения. Поиск новых решений в данном направлении является одним из главных трендов в области информационной безопасности в 2023 году. Рассматриваются комплексные решения, основанные на синтезе традиционных существующих мер от данных типов цифровых рисков, программ по управлению внешней поверхностью кибератаки и иными средствами. Новые решения чрезывайно актуальны, так как и киберпреступники применяют новые инструменты и технологии. Можно выделить атаки через Open Source и написанный на кросс-платформенных языках вредоносный код. Опасны атаки посредством вайперов, шифровальщиков и инфостилеров. Необходимость активного импортозамещения программного обеспечения. требует разработок "с нуля", однако начальная разработка предусматривает наличие множества уязвимостей на начальных этапах, требуется длительное тестирование и проверка эксплуатации на выявление возможных сбоев и уязвимостей. Информационная безопасность, таким образом, имеет сильную зависимость от скорости принятия и внедрения российскими компаниями новых технологий, инструментов и моделей, обеспечивающих информационную безопасность. Zero Trust – модель нулевого доверия, при которой новый пользователь или подключенное устройство вынуждены доказывать свое право на доступ при помощи полной идентификации. Распределенные доступы и многоуровневая идентификация позволяют службе безопасности компании вместе с ИИ лучше защищать внутреннюю систему от злоумышленников. Особое внимание уделяется разработкам **Zero Trust и Threat Hunting.**

Zero Trust – модель, в которой каждый новый пользователь или подключенное устройство должны пройти полную идентификацию для получения доступа. Threat hunting – обеспечение проактивного поиска следов взлома или проникновения вредоносных программ при отсутствии их обнаружения при помощи стандартных средств защиты [5].

Таким образом, комплексный подход к обеспечению минимизации угроз информационной безопасности предусматривает активное законодательное обновление существующих условий правового свойства в данном секторе, оперативное внедрение жизнеспособных стартапов в сфере информационной безопасности, способных обеспечить импортозамещение технологий и инструментов в этой области, быстрое и качественное обучение необходимых кадров и четкий контроль за происходящими изменениями.

Список использованных источников

1. Евдокимова, А. А. Сферы и направления применения искусственного интеллекта в банках / А. А. Евдокимова, Ю. В. Евдокимова // Инвестиционный климат и искусственный интеллект: взаимосвязи и проблемы трансформации мегаполиса : сб. науч. трудов; под ред. А. А. Шестемирова, Ю. В. Евдокимовой. – М., 2022. – С. 14–18.

2. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации [Электронный ресурс] : Указ Президента Российской Федерации, 1 мая 2022 г. № 250 // Справочно-правовая система Консультант Плюс. Россия / ЗАО «Консультант Плюс».

3. Защита информации. Идентификация и аутентификация. Уровни доверия идентификации : ГОСТ Р 70262.1-2022 // Справочно-правовая система Консультант Плюс.Россия / ЗАО «Консультант Плюс».

4. О внесении изменений в Федеральный закон "О персональных данных": Федер. закон, 14.07.2022 г. № 266-ФЗ // Справочно-правовая система Консультант Плюс. Россия. / ЗАО «Консультант Плюс».

5. Что такое threat hunting, и как правильно охотиться на киберпреступников [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/pt/articles/510362/. – Дата доступа: 14.09.2023.

References

1. Evdokimova, A. A. Sfery i napravleniya primeneniya iskusstvennogo intellekta v bankah / A. A. Evdokimova, Yu. V. Evdokimova // Investicionnyj klimat i iskusstvennyj intellekt: vzaimosvyazi i problemy transformacii megapolisa : sb. nauch. trudov; pod red. A. A. Shestemirova, Yu. V. Evdokimovoj. – M., 2022. – S. 14–18.
2. O dopolnitel'nyh merah po obespecheniyu informacionnoj bezopasnosti Rossijskoj Federacii [Elektronnyj resurs] : Ukaz Prezidenta Rossijskoj Federacii, 1 maya 2022 g. № 250 // Spravochno-pravovaya sistema Konsul'tant Plyus. Rossiya / ZAO «Konsul'tant Plyus».
3. Zashchita informacii. Identifikaciya i autentifikaciya. Urovni doveriya identifikacii : GOST R 70262.1-2022 // Spravochno-pravovaya sistema Konsul'tant Plyus.Rossiya / ZAO «Konsul'tant Plyus».
4. O vnesenii izmenenij v Federal'nyj zakon "O personal'nyh dannyh": Feder. zakon, 14.07.2022 g. № 266-FZ // Spravochno-pravovaya sistema Konsul'tant Plyus. Rossiya. / ZAO «Konsul'tant Plyus».
5. Chto takoe threat hunting, i kak pravil'no ohotit'sya na kiberprestupnikov [Elek-tronnyj resurs]. – Rezhim dostupa: https://habr.com/ru/companies/pt/articles/510362/. – Data do-stkpa: 14.09.2023.

УДК 338:324

ОПЫТ ФУНКЦИОНИРОВАНИЯ КРУПНЫХ СТРОИТЕЛЬНЫХ ОРГАНИЗАЦИЙ В РОССИИ

Е. А. Жукова
Научный руководитель: Н. В. Носко

Брестский государственный технический университет
Республика Беларусь, г. Брест, ул. Московская, 267
katya.zhukova.04@gmail.com

В данной статье рассмотрен опыт функционирования крупных строительных организаций в России, выявлены особенности функционирования и состав строительного комплекса, также приведены статистические данные о строительных организациях в России, рассмотрены формы собственности, формы корпоративных объединений и стратегия развития строительной отрасли и ЖКХ в России.

Ключевые слова: строительные организации, строительный комплекс, формы собственности, формы корпоративных объединений, региональные различия, стратегия развития, жилищное строительство.

OPERATING EXPERIENCE OF LARGE CONSTRUCTION ORGANIZATIONS IN RUSSIA

E. A. Zhukova
Supervisor: N. V. Nosko

Brest State Technical University
Republic of Belarus, Brest, Moskovskaya str., 267
katya.zhukova.04@gmail.com

This article examines the experience of functioning of large construction organizations in Russia, identifies the features of the functioning and composition of the construction complex, also provides statistical data on construction organizations in Russia, examines the forms of ownership,