УДК 004.056

Современные угрозы информационной безопасности предприятия и их классификация

Лукина Анастасия Юрьевна
Нижегородский институт управления РАНХиГС
Студент

Аннотация
Статья посвящена исследованию основных угроз информационной безопасности субъектов экономики и государства. В ходе работы автором определен понятийный аппарат информационных систем и технологий. Проанализировано современное состояние использования информации в экономическом и социальном секторе РФ и его влияние на экономическую и национальную безопасность страны. По итогу работы на основании теоретического материала и практических исследований современных ученых предложена авторская классификация информационных угроз предприятия.
Ключевые слова: информационная безопасность, национальная безопасность, экономика, общество, воздействие.

Modern information security threats to the enterprise and their classification

Lukina Anastasiya Urevna
Nizhny Novgorod Institute of Management RANEPA
Student

Abstract
The article investigates the main threats to information security subjects of the economy and the state. During the work the author defined the conceptual apparatus of information systems and technologies. The current state of the use of information in the economic and social sector of the Russian Federation and its impact on the economic and national security. According to the results of work on the basis of theoretical material and practical research of modern scientists offered author's classification of information threats companies.
Keywords: information security, national security, economy, society, impact.

Текущие изменения концепций и структур информационного общества и цифровой экономики в мире не только расширяют круг новых возможностей для развития экономических субъектов, но и опосредованно влияют на появление соответствующих угроз безопасности данных субъектов. Так, социальные институты, предприятия разных сфер деятельности и форм собственности, а также государственные управленческие аппараты разных стран на данном историческом этапе

глобализации и информатизации характеризуются активным функционированием и динамичным преобразованием структуры информационных данных, с чем связана актуальность выбранного направления исследования.

Целью данной статьи является определение угроз информационной безопасности предприятия и их классификация, а также обозначение ключевых принципов противодействия негативному информационному воздействию на безопасность экономики субъекта и государства в целом.

Информационные данные и технологии постепенно видоизменяют привычные процессы взаимодействия в обществе, продуцируют появление новых качеств и концепций в экономическом развитии стран и отдельных субъектов хозяйствования [2]. Говоря о глобальном измерении в распространении и воздействии информации, следует также выделить возможность повышения уровня конкурентоспособности отдельной страны на международном рынке посредством создания прочного технологического фундамента перманентных трансформаций экономики [1].

Кроме невиданных ранее возможностей для повышения материального благосостояния обществ, современные информационные технологии и их повсеместное распространение повлекло за собой проявление принципиально новых моделей экономического взаимодействия, социальной интеграции и т.д.

Поскольку мир перешел от физического к цифровому ландшафту, угрозы безопасности также изменились с физического воздействия на информационное. Так, согласно исследованию компании Juniper, сумма ущерба от информационных атак для глобальной экономики в 2019 году составила 2 триллиона долларов. По оценкам специалистов, к 2027 году глобальные расходы экономических структур всех государств на информационную безопасность достигнут 10 миллиардов долларов. Кроме того, также исследованиями компании Juniper отмечается, что половина всех кибератак направлена на малый бизнес [9].

В пресс-релизе Global Market Insights за 2019 год указывалось, что к 2024 году ожидается, что рынок информационной безопасности станет отраслью с оборотом в 300 миллиардов долларов [8].

Современная политика государства относительно развития информационных технологий в РФ базируется на таких принципах:

- ключевым направлением инноваций любой отрасли хозяйствования становится научно-технический прогресс;
- законодательно подкрепляется и экономически поощряется применение новых информационных технологий [7];
- изменяется со временем понятие доступности информации – информационные технологии и базы информационных данных становятся компонентой общественного функционирования и экономического развития государства;

- реализуется концепция искоренения бюрократических проявлений посредством перехода на электронный документооборот в бюджетных и коммерческих организациях;
- ИТ внедряются в общественную жизнь и все ее ключевые звенья (первично – в экономическую систему страны) [5];
- государством гарантируется информационной безопасности [6].

Непосредственно дефиниция «информационная безопасность» отражает в целом состояние информационной защиты хозяйствующего субъекта в условиях, когда существует вероятность угроз. Информационная безопасность предприятия может быть достигнута посредством применения комплекса мер, направленных на предупреждение, выявление и ликвидацию информационных угроз [4]. Спектр интересов информационной безопасности предприятия как объектов безопасности предлагаем разделить на следующие основные категории:

- доступность - возможность за определенное время получить определенную информационную услугу;
- целостность - релевантность и однозначность информации, ее защищенность от разрушения и несанкционированного изменения;
- конфиденциальность - защищенность от несанкционированного доступа.

С позиции механизмов и методологий защиты информации экономического субъекта информационная безопасность представляет собой целостную концепцию, которая позволяет выявлять уязвимые места информационно-коммуникативной системы предприятия, опасности, которые угрожают ей, и методы нейтрализации выявленных угроз. Угрозой признается событие, которое может вызвать нарушение функционирования информационной системы, включая искажение, полное уничтожение или несанкционированное применения данных соответствующего субъекта [3].

Анализируя подходы отечественных исследователей к классификации угроз информационной безопасности, следует констатировать, что унифицированный подход отсутствует. Обобщая и аналитически интерпретируя позиции современных авторов, предлагаем следующую авторскую классификацию угроз:

1. В соответствии с проявлением и последствиями: преступление; мошенничество; хулиганство.
2. В соответствии с типом воздействия: программные; аппаратные и пр.
3. В соответствии с целью воздействия: оперативные, тактические, стратегические.
4. В соответствии с характером возникновения: преднамеренные, непреднамеренные.
5. В соответствии с видом ИТ: объект угроз, методы подготовки угроз, инструментарий угроз, среда угроз.
6. В соответствии с местом возникновения: инсайдерские, внешние.
7. В соответствии с объектом воздействия: системные, локальные.

8. В соответствии с причиной возникновения: сбои в оборудовании, сбои в работе программного обеспечения, несовершенная архивация данных, несанкционированный доступ.

Таким образом, развитие информационных технологий и средств коммуникаций обеспечивают все более широкие возможности доступа к информационным ресурсам и перемещения больших массивов данных на неограниченные расстояния. При этом доступ широкого круга пользователей, место нахождения которых может быть произвольным, к ресурсам, которые находятся в рамках глобальной информационной сети, увеличивает число и вариации угроз информационным ресурсам и информационной системе предприятия. В связи с указанным, информация как продукт, имеющий спрос, нуждается в сохранении и надежной защите.

Ключевым направлением концептуальных сдвигов на современных предприятиях должно стать понимание руководителями и сотрудниками роли собственной социально-экономической ответственности в системе обеспечения информационной безопасности отдельной организации и страны в целом. Что же касается мероприятий, которые являются необходимыми в структуре избегания субъектом предпринимательства внешних и внутренних посягательств (угроз) на информационные данные, то здесь стоит выделить такие компоненты системы безопасности, как: перманентный мониторинг состояния безопасности, своевременное выявление угроз (как реально существующих, так и намеченных в перспективе стратегией безопасности), комплексная оценка и предотвращение специалистами угроз. Кроме того, сотрудникам или ответственным лицам системы информационной безопасности предприятия необходимо оперировать понятиями и владеть знаниями области социальной инженерии, чтобы своевременно обеспечивать защиту конфиденциальной информации от несанкционированного доступа, предотвращать посягательства или случайные изменения информационных данных (контролировать целостность и сохранность) и давать необходимый уровень доступа соответствующему кругу пользователей. Обеспечение информационной безопасности сводится к трем основным направлениям, которые являют собой комплекс технических, административных и организационных мер.

Таким образом, в современных условиях хозяйствования, когда информационные технологии приобретают глобальный характер, информационная безопасность является неотъемлемой составляющей системы экономической безопасности хозяйствующего субъекта и экономической, а также национальной безопасности государства в целом.

Библиографический список

1. Круглякова А.Д. Информационная безопасность, как одна из угроз национальной безопасности Российской Федерации непосредственный // Актуальные вопросы науки. 2019. №. 50. С. 162-164.
2. Лось Л.В. Информационная безопасность в системе национальной

безопасности Российской Федерации // Вопросы российского и международного права. 2019. Т. 9. № 3-1. С. 159-170.
3. Палагин Р.А. Информационная безопасность в системе обеспечения экономической и национальной безопасности России // Мировая наука. 2019. № 5 (26). С. 551-556.
4. Полыхань К.О. Проблемы и особенности состояния информационной безопасности в соответствии с доктриной информационной безопасности РФ // Устойчивое развитие науки и образования. 2019. № 5. С. 154-160.
5. Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» от 09.05.2017 № 203 // Консультант плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 16.04. 2020).
6. Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 № 646 // Консультант плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 16.04.2020).
7. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 03.04.2020) // Консультант плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 15.04.2020).
8. Cyber Security Statistics 2019. // Cyberbit. 2019. URL: https://www.cyberbit.com/blog/cybersecurity-training/cyber-security-statistics-2019/ (дата обращения: 16.04.2020).
9. Cybercrime will cost businesses over $2 trillion by 2019. // Juniper Research Ltd and its licensors. 2019. URL: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019 (дата обращения: 16.04.2020).