УДК 004

Хафизова Л.Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

СОВРЕМЕННЫЕ УГРОЗЫ И УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАСТИ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ

Аннотация. Статья посвящена анализу современных угроз и уязвимостей информационной безопасности в области организационной защиты. С развитием технологий и цифровизации бизнеса, компании сталкиваются с растущими рисками, связанными с утечкой конфиденциальной информации, кибератаками, внутренними угрозами и другими проблемами.

Ключевые слова: информация, информационная безопасность, угрозы, организационные угрозы, уязвимости, организационные уязвимости, информационные технологии, защита информации, организационная защита.

Угрозы информационной безопасности (ИБ) часто являются следствием уязвимостей в самой системе защиты информации. Такие уязвимости могут возникать по разным причинам. Это могут быть случайные ошибки, допущенные специалистами при разработке или сопровождении программного обеспечения, а могут быть и намеренные действия – например, целенаправленная кража данных или внедрение вредоносного кода.

При рассмотрении таких угроз принято разделять их на две категории – технические и организационные. Технические включают в себя физиические и программные уязвимости на информационные системы. Организационные же, в свою очередь, связаны прежде всего с человеческим фактором – с действиями персонала и управленческими просчетами.

Несмотря на такую классификацию, во многих существующих подходах к анализу ИБ основное внимание уделяется именно технологическим аспектам безопасности. Организационные угрозы, напротив, часто остаются в стороне – их влияние недооценивают или не всегда принимают в расчет. Однако практика показывает, что именно они могут представлять серьезную опасность для устойчивости и защищенности ИС. Поэтому специалисты по информационной безопасности все чаще разрабатывают собственные классификации угроз, в которых наравне с техническими подробно рассматриваются и организационные риски.

Организационные угрозы могут проявляться в разных формах. Иногда это внешнее влияние на сотрудников со стороны третьих лиц – давление, манипуляции или даже угрозы. Воздействие может быть, как физическим, так и психологическим. Нередко бывает так что угрозы исходят от самих сотрудников – намеренно или по ошибке. Кто-то может сознательно нарушать правила безопасности, действуя из личной заинтересованности или по заказу, а кто-то, не имея достаточной квалификации или по невнимательности, допускает серьезные ошибки.

Таким образом, можно сказать, что организационные угрозы либо направлены на персонал, либо реализуются через него. Сотрудники компании могут быть как объектом, так и источником угроз информационной безопасности. Именно поэтому человеческий фактор играет ключевую роль в обеспечении устойчивой и надежной защиты информации.

Физическое воздействие на сотрудников предполагает применение силы или угроз, чтобы заставить человека – напрямую или через посредников – раскрыть конфиденциальную информацию либо нарушить работу процессов внутри компании. Подобные инциденты относятся к категории серьезных нарушений и, как правило, становятся предметом расследования со стороны службы ИБ, а также правоохранительных органов.

На практики существует более гибкая угроза, но не менее опасная – психологическое воздействие. В этой категории широко используются такие методы, как шантаж, подкуп, манипулирование, а также приемы социальной инженерии. Все они направлены на то, чтобы повлиять на поведение человека и получить от него нужные действия или информацию без применения технических средств.

Особенно стоит отметить методы социальной инженерии. Они представляют особую опасность, поскольку базируются на умении злоумышленника использовать человеческую психологию. Часто достаточно лишь изучить структуру компании, позвонить в отдел, представиться сотрудником или поставщиком – и можно получить доступ к внутренним данным. Нередко злоумышленники прибегают к хитростям: несанкционированный доступ в компьютер, через незакрытые USB-порты или возможности подключения устройств.

Именно поэтому в организациях все чаще внедряют системы контроля и управления доступом (СКУД). Эти меры позволяют ограничить вход на территорию, вести учет передвижений и минимизировать риски, связанные с социальной инженерией.

Среди методов психологического давления выделяется манипуляция – умелое управление поведением человека, при котором у него формируется желание действовать в интересах другого, зачастую вопреки своей воле. Такие воздействия могут быть неочевидны, но в итоге приводят к выполнению нежелательных действий.

Психологическая атака – это еще более активный способ влияния. Злоумышленник может создать у человека состояние замешательства, срочности или сильного впечатления, чтобы временно отключить логическое мышление. В результате сотрудник действует автоматически и совершает поступки, которых от него добивается атакующий.

Однако ни одна атака не осуществляется в пустоте – всегда требуется определенная уязвимость. Чтобы провести успешную информационную атаку, злоумышленник должен использовать слабое место в системе. Если эти уязвимости своевременно устранять или минимизировать, вероятность реализации угроз заметно снижается.

Особенно уязвимыми считаются организационные слабости, связанные с человеческим фактором. Они могут проявляться как через сотрудников компании, так и через подрядчиков или партнеров. Чаще всего это недостаток подготовки, слабая мотивация, нехватка контроля и отсутствующие знания по ИБ.

Если сотрудники не обучены, не знают правил или не понимают последствий своих действий – они становятся легкой мишенью. А при отсутствии внутреннего мониторинга, риски возрастают в разы, ведь инциденты остаются незамеченными.

Чтобы устранить подобные уязвимости, организациям необходимо регулярно обучать персонал, знакомить их с актуальными методами защиты, повышать квалификацию. Также большую роль играет нематериальная мотивация: сотрудник должен понимать, что его труд ценится не только финансово, но и на уровне признания со стороны руководства. Это помогает формировать ответственное отношение к вопросам безопасности.

Помимо этого, необходимо создать систему мониторинга, которая позволит отслеживать соблюдение правил и выявлять отклонения. Каждый сотрудник должен понимать свои обязанности, знать регламенты и последствия их нарушения.

Современные организационно-технические мероприятия должны включать в себя:

1. Контроль доступа к информации с помощью установления прав доступа к системе и данным.
2. Шифрование информации для защиты от несанкционированного доступа.
3. Аудит безопасности для мониторинга действий пользователей и выявления угроз.
4. Резервное копирование данных для обеспечения возможности восстановления после инцидентов.

Однако с техническими мерами не стоит забывать организационно-правовые. Это разработка внутренних политик безопасности, инструкций и регламентов. Важно, чтобы все сотрудники знали, что можно, а что нельзя,

и кто за что отвечает. Такие документы должны быть не формальностью, а реально работающим инструментом.

К сожалению, на практике основная проблема – это отсутствие элементарных документов. Если в компании нет утвержденной политики ИБ, сотрудники действуют на свое усмотрение. А это уже прямая дорога к инцидентам.

В целом, можно сказать, что организационные уязвимости чаще всего возникают не из-за отсутствия средств, а из-за отсутствия порядка, контроля и культуры безопасности. Если наладить эти процессы – ввести регламенты, обучить сотрудников, назначить ответственных – уровень защиты значительно возрастет.

Важно помнить: большинство организационных угроз связаны с персоналом. Это может быть, как внешнее воздействие, так и действия самих сотрудников. Поэтому эффективная защита информации невозможна без вовлечения людей, их подготовки, осознанности и ответственности.

Список использованных источников:

1. Гаценко О.Ю. Защита информации: основы организационного управления: учебное пособие / О.Ю. Гаценко. Сентябрь, 2011. 228 с.

2. Романов О.А. Организационное обеспечение информационной безопасности: учебник для высших учебных заведений / О.А. Романов. М.: Академия, 2008. 192 с.

3. Семкин С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие / С.Н. Семкин. М.: Гелиос АРВ, 2010. 185 с.

4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: учебник для высших учебных заведений / А.А. Стрельцов. М.: Академия, 2008. 248 с.

Khafizova L.F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

MODERN THREATS AND VULNERABILITIES OF INFORMATION SECURITY IN THE FIELD OF ORGANIZATIONAL PROTECTION

Abstract. The article is devoted to the analysis of modern threats and vulnerabilities of information security in the field of organizational protection. With the development of technology and digitalization of business, companies

face increasing risks associated with confidential information leaks, cyber attacks, internal threats and other problems.

Keywords: information, information security, threats, organizational threats, vulnerabilities, organizational vulnerabilities, information technology, information security, organizational protection.