Чуприк Александр Александрович
студент
ФГБОУ ВО «Санкт-Петербургский государственный
архитектурно-строительный университет»
г. Санкт-Петербург

ЧЕЛОВЕЧЕСКИЙ ФАКТОР КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Аннотация*: в настоящие время существует повышенный спрос к такой проблеме, как человеческий фактор в информационной безопасности организации. Сотрудники организации слабейшие звенья в цепочки информационной безопасности организации из-за своей уязвимости, человеческий фактор играет основную роль в этой проблеме. Зачастую это является непреднамеренной ошибкой, и сотрудник создает утечку данных без злого умысла, зачастую сотрудники не осведомлены, как пользоваться тем или иным ПО, оборудованием или не соблюдают стандартные правила информационной безопасности: не обновляют программное обеспечение, не соблюдают правила безопасности при работе с онлайн-банкингом и другими финансовыми сервисами, пользуясь доверчивостью штата сотрудников или с помощью манипуляций пользуясь навыками социальной инженерии конкуренты или мошенники (киберпреступники), получают конфиденциальную информацию, сотрудников, клиентов, поставщиков или иной ценной информации.*

Ключевые слова*: информационная безопасность, работа с персоналом, безопасность, аналитика.*

Человеческий фактор является одним из ключевых аспектов информационной безопасности. Он включает в себя все аспекты, связанные с поведением и действиями людей, которые могут повлиять на безопасность информации, систем и сетей.

Основными угрозами, связанными с человеческим фактором, являются: Ошибки и упущения при выполнении задач: Люди могут случайно или намеренно

нарушить правила безопасности, такие как несоблюдение паролей, ненадлежащее использование общих ресурсов и т. д. Технические уязвимости: сотрудники могут использовать уязвимости в программном обеспечении или неправильно настроить оборудование, что может привести к утечке информации или нарушению работоспособности систем. Злоупотребление полномочиями: сотрудники могут использовать свои привилегии для доступа к конфиденциальной информации или выполнения несанкционированных действий, таких как кража данных или взлом систем. Недостаток образования и осведомленности: недостаточное обучение сотрудников в области информационной безопасности может привести к тому, что они не будут знать о существующих угрозах и как их предотвратить. Социальная инженерия: мошенники могут использовать различные методы, чтобы обмануть сотрудников и получить доступ к важной информации, фишинг или вирусы, которые могут использоваться для нарушения безопасности систем и данных. Усталость и стресс: из-за высокого уровня стресса и усталости сотрудники могут совершать ошибки или принимать неверные решения, которые негативно сказываются на безопасности информации и эмоциональное выгорание может снижать эффективность работы и повышать вероятность ошибок.

Для предотвращения этих угроз необходимо проводить обучение и повышение квалификации сотрудников, внедрять системы контроля и мониторинга, а также разрабатывать и применять мотивационные программы для поддержания высокого уровня безопасности и эффективности работы.

Виды борьбы с информационными угрозами на предприятии. Антивирусные программы:(*McAfee, ESET Smart Security Premium, Sophos Home Premium*). Защита от *DDoS*-атак (*Cloudflare, Project Shield, AWS Shield*). Специализированные средства по защите от целевых атак (*PT Sandbox, PT Network Attack Discovery, Xello Deception*).

Один из способов повысить информацию безопасность предприятия – это мотивация сотрудников; нужно монтировать сотрудников на безопасную работу в информационном поле.

1. Получение премии для сотрудников отдела, у которых отсутствовали утечки данных за тот или иной период.

2. Проведения проверки информационной безопасности компании, то есть проверка почты организации когда; производиться очистка и блокировка спам контента вручную и через специальное антивирусное ПО за такую проделанную работу сотрудник будет получать премию.

3. Выдача дополнительного выходного дня раз в месяц и компенсация за покупку антивирусного ПО на свое личное устройство для обеспечения информационной безопасности предприятия в не офиса актуально для работников, работающих на аутсорсинге и работников которых состоят в штате, но работают удаленно.

Второй способ повысить информационную безопасность предприятия это осведомленность сотрудников многие сотрудники могут не знать, как различить спам и вредоносные ссылки, и ПО от коммерческой информации.

1. Нужно проводить специальные тренинги и курсы и по повышению квалификации в этой сфере чтобы сотрудники были осведомлены о возможных угрозах и могли предотвратить их.

2. Подписания NDA (соглашение о неразглашении конфиденциальной информации) при приеме сотрудников на работу это повысить отвесность работников при работе с информацией и предотвратит возможную утечку данных, а в случае утечки сотрудник будет нести отвесность в случаи утечки.

1. Безопасность беспроводных сетей: использование защищенных беспроводных соединений и шифрование данных при использовании *Wi-Fi*.

2. Обновление программного обеспечения: своевременное обновление программного обеспечения на компьютерах и мобильных устройствах сотрудников.

3. Установка антивирусного программного обеспечения: использование антивирусных программ для защиты компьютеров и мобильных устройств сотрудников от вредоносного ПО.

4. Внедрение системы контроля доступа: установка системы контроля доступа для ограничения доступа к конфиденциальной информации на предприятии.

5. Шифрование данных: использование шифрования данных для защиты информации от несанкционированного доступа. На предприятии шифрование данных может быть реализовано с помощью различных инструментов и технологий. Например, можно использовать встроенные функции операционной системы или специальные программные средства для шифрования файлов и папок.

6. Мониторинг сети: регулярный мониторинг сети предприятия для обнаружения и предотвращения сетевых атак, Сбор и анализ данных и журналов с сетевых устройств для выявления тенденций, определения проблем и оптимизации производительности и эффективности сети.

Рассмотрим экономическую составляющую человеческого фактора как угрозы информационной безопасности более подробно: 1. Прямые финансовые потери – кража денежных средств, финансовых данных или возможность незаконного перевода средств из-за действий инсайдера или в результате социальной инженерии; – потеря интеллектуальной собственности, ценных данных, приводящая к утрате конкурентных преимуществ; – затраты на восстановление систем, данных после инцидента безопасности; – судебные издержки, компенсации, штрафы в связи с инцидентами. 2. Косвенные финансовые потери – упущенная выгода из-за простоя операций, сбоев производства в результате атак или инцидентов; – потеря клиентов и репутационный ущерб, ведущий к снижению доходов в долгосрочной перспективе; – затраты на восстановление репутации, маркетинговые компании после утечек данных; – ущерб бренду компании, снижение стоимости акций из-за потери доверия клиентов и инвесторов. 3. Затраты на меры предотвращения – расходы на обучение персонала, повышение осведомленности в сфере ИБ; – внедрение систем контроля доступа, шифрования, резервного копирования и т. д.; – привлечение специалистов по ИБ, консультантов для оценки рисков; – страхование кибер-рисков для покрытия возможных потерь. 4. Упущенные возможности – перенаправление ресурсов (финансовых, трудовых) на устранение последствий инцидентов; – отставание от конкурентов из-

за нарушений производственных процессов; – сложности в привлечении инвестиций и ведении бизнеса из-за репутационных потерь.

Таким образом, человеческий фактор может оказывать существенное негативное влияние на экономику предприятия как напрямую, так и косвенно через нарушение операционной деятельности, потери нематериальных активов и упущенные возможности. Грамотная оценка и управление этими рисками является важной задачей обеспечения финансовой устойчивости бизнеса.

Список литературы

1. Дубинина Н.А. Подходы к оценке сбалансированности развития предприятий / Н.А. Дубинина, В.В. Усков // Вестник Астраханского государственного технического университета. Серия: Экономика. – 2019. – №1. – С. 164–172.

2. Моденов А.К. Оценка риска в экономической безопасности предприятия: учебное пособие / А.К. Моденов, М.П. Власов, Т.Н. Орловская [и др.]. – в 2 ч. – СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2022. – 257 с. – ISBN 978–5-7422–7795–8. – EDN BVGUMW.

3. Vlasov M.P. Modelling of the supply chain planning for the business and economic security / M.P. Vlasov, A.K. Modenov, O.V. Harchenko // International Journal of Supply Chain Management. – 2020. – Vol. 9. №3. – P. 750–756. – EDN GQPUUB.