

Информационные технологии (ИТ) представляют неотъемлемую часть жизни современного человека. Данные технологии работают на базе использования множества средств и методов сбора, обработки, а также передачи данных с целью получения информации необходимого качества и состоянии какого-либо объекта, процесса или явления из энергетической отрасли. Основной целью информационных технологий является усовершенствование и автоматизация производственных процессов на предприятии. Информационные технологии являются лидирующим направлением в профессиональной сфере человека. Повсеместно внедряются и разрабатываются совершенно новые и ранее неизученные технологии. На современных предприятиях происходит интенсивное распространение с совместным совершенствованием цифровых и информационных технологий. Данное направление в течение длительного времени определяет основные траектории развития экономики и общества, а также уже не один раз приводило к колоссальным изменениям, касающимся жизни людей.

Цифровые и информационные технологии – это важнейшая часть современных систем управления, находящихся во всех отраслях экономики на сегодняшний день. Следствием данного фактора является появление новых кибер-угроз и кибератак, совершаемых в областях, в основе которых функционируют различные информационные системы и иные информационные технологии. В современном мире складывается тенденция роста количества попыток совершения киберпреступлений на объектах критически важной информационной инфраструктуры (КИИ) с помощью использования информационно-коммуникационных технологий (ИКТ) .

Критически важными информационными инфраструктурами являются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия. Компьютерная атака на КИИ определяется как целенаправленное вредоносное воздействие на объекты КИИ для нарушения или прекращения их функционирования, а компьютерное происшествие в качестве факта нарушения или же прекращения функционирования объекта КИИ или нарушения безопасности обрабатываемой объектом информации.

Категория значимости объекта критически важной информационной инфраструктуры может принимать одно из трех значений (где самая высокая категория - первая, самая низкая - третья) и зависит от количественных показателей значимости этого объекта в социальной, политической, экономической и оборонной сферах. Процесс категорирования данных объектов проводится внутренней комиссией по категорированию субъекта КИИ, в

результате чего формируется список объектов КИИ с категориями значимости и затем отправляется в ФСТЭК России, где полученные сведения вносятся в специальный реестр объектов КИИ. Таким образом, категорирование КИИ состоит из нескольких взаимосвязанных шагов, результатом которых является составление субъектом КИИ Акта категорирования КИИ и наполнение реестра объектов КИИ данными с соответствующими категориями значимости.

Множественные удачные попытки подобного рода преступлений свидетельствуют о том, что посредством ИКТ действительно можно нанести колоссальный как физический, так и информационный ущерб. Необходимо отметить, что при нахождении киберпреступником уязвимости в одном из компонентов информационной системы на критически важных объектах, представляется возможным осуществление целенаправленных нападений на объекты по всему миру .

Необходимо отметить, что игнорирование возникающих проблем способно привести к потере конкурентоспособности как на государственном, так и на корпоративном уровне. Также от преступлений в информационной сфере страдают не только организации и предприятия, но и обычные граждане, пользующиеся гаджетами и иными средствами коммуникации.

Актуальность угрозы целостности информационных ресурсов требует внимание в отношении задач по ее защите. Стоит отметить, что 20 лет назад задача, связанная с обеспечением информационной безопасности, решалась посредством применения алгоритмов шифрования, установления межсетевых экранов, разграничения доступа и так далее. На сегодняшний день данных технологий недостаточно, именно поэтому практически любая информация, имеющая финансовый, конкурентный, военный или политический характер подвергается угрозе. Также дополнительным риском является возможность перехвата управления критическими объектами информационной инфраструктуры.

Исходя из этого, на современных объектах КИИ особую актуальность приобретают задачи, решение которых направлено на своевременное обновление базовых компонентов систем управления. Также стоит отметить, что на сегодняшний день не только со стороны производителей, но и со стороны самих потребителей не всегда уделяется должное внимание вопросу кибербезопасности. Совокупность данных факторов приводит к развитию новых методов и угроз нарушения безопасности.

Таким образом, посредством информации и информационных технологий передаются конфиденциальные данные, производятся транзакции на различных предприятиях, производится хранение и работа с засекреченной информацией и так далее. Данный список можно перечислять бесконечно, так как в век информационных технологий практически все процессы, происходящие в жизнедеятельности человека, основываются на применении информационных технологий и информации, в частности. Исходя из этого формируется проблема, связанная с защитой информации и информационных ресурсов в целом. Информационная безопасность является одной из ключевых и приоритетных направлений на сегодняшний день. Каждые полгода количество атак на информационные ресурсы предприятий растет на 4-5%. Также стоит отметить, что с ростом числа нарушений снижается доля их раскрываемости, которая не превышает 41%.

Исходя из вышеперечисленных факторов, вопрос обеспечения информационной безопасности на объектах КИИ имеет достаточно высокую актуальность. На сегодняшний день должно уделяться намного большее внимание, касаясь данного вопроса. Недостаточный уровень развития информационной безопасности подобных объектов способен привести к колоссальным последствиям для экономики не только одной страны, но и всего мира.

## Список литературы

1. Лебедь В.Н., Терещенко Б.И., Восканян К.А. Управление процессами обеспечения кибербезопасности как фактор международной стабильности // Коммуникология: электронный научный журнал. 2017.
2. Ковалев А. А., Балашов А. И. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока // Вестник ПАГС. 2018.
3. Garin E.V. Foreign experience of using artificial intelligence technologies in ensuring information security of the banking sector // The territory of new opportunities. 2019.