УДК 004.9

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Разнатовский К.К. – студент гр.17В41,
Научный руководитель: Е.В. Телипенко, к.т.н. доцент
Юргинский технологический институт (филиал)
Национального исследовательского Томского
политехнического университета
Россия, г. Юрга

Информация в XXI веке стала ключевым активом, новой «нефтью». От персональных данных пользователей социальных сетей до коммерческой тайны крупных корпораций и государственных секретов — все это циркулирует в цифровом пространстве. Стоимость утечки или компрометации этой информации измеряется не только в прямых финансовых потерях, но и в репутационном ущербе, судебных издержках и утрате конкурентных преимуществ. Таким образом, информационная безопасность — это не просто набор технологий, а комплексная дисциплина, направленная на обеспечение конфиденциальности, целостности и доступности информации.

Конфиденциальность гарантирует, что информация доступна только тем субъектам, которые имеют на это право. Целостность обеспечивает точность и полноту данных, защищая их от несанкционированного изменения. Доступность гарантирует, что авторизованные пользователи имеют доступ к информации и связанным с ней активам, когда это необходимо.

Триада «конфиденциальность-целостность-доступность» (CIA — Confidentiality, Integrity, Availability) является краеугольным камнем любой системы информационной безопасности.

Часть 1: Эволюция киберугроз — от вирусов до целевых атак

Угрозы информационной безопасности постоянно эволюционируют, становясь все более изощренными, масштабными и опасными.

От «вандализма» к коммерциализации. Если первые компьютерные вирусы создавались ради «спортивного интереса» или демонстрации навыков, то современное киберпреступность — это высокодоходный бизнес. Появились целые экосистемы, включающие в себя поставщиков вредоносного ПО (Ransomware-as-a-Service), сервисы для организации DDoS-атак и рынки по продаже украденных данных.

Целевые атаки и APT (Advanced Persistent Threat). В отличие от массовых атак, целевые кампании направлены на конкретную организацию или государственную структуру. Злоумышленники (часто спонсируемые государствами) проводят тщательную разведку, используют социальную инженерию и

нулевые уязвимости (zero-day), чтобы месяцами оставаться незамеченными внутри корпоративной сети, похищая критически важную информацию.

Социальная инженерия и фишинг. Человеческий фактор остается самым слабым звеном в системе безопасности. Фишинговые письма, имитирующие сообщения от банков или коллег, звонки от «техподдержки» и другие методы манипуляции позволяют злоумышленникам обойти даже самые сложные технические средства защиты.

Угрозы для интернета вещей (IoT). Миллиарды подключенных устройств — от камер видеонаблюдения до промышленных систем управления — создают новую, плохо защищенную поверхность для атак. Компрометация IoT-устройств может привести не только к утечке данных, но и к физическому ущербу.

Ransomware (Вымогатели). Эта угроза выделяется в отдельную категорию из-за своей разрушительности. Вредоносное программное обеспечение шифрует данные жертвы с требованием выкупа за их расшифровку. В последние годы атаки стали двойными: данные не только шифруются, но и похищаются, чтобы в случае отказа от выплаты быть опубликованными в даркнете.

Часть 2: Комплексный подход к защите: технологии, процессы, люди

Построение эффективной системы информационной безопасности требует комплексного подхода, который часто описывают моделью «Технологии — Процессы — Люди».

1.Технологический фундамент
Это базовый уровень защиты, включающий в себя:

Межсетевые экраны (Firewalls) и системы обнаружения/предотвращения вторжений (IDS/IPS): контролируют и фильтруют сетевой трафик.

Антивирусное ПО и средства защиты от вредоносных программ: обнаруживают и нейтрализуют известные угрозы.

Системы шифрования: защищают данные как при хранении (на дисках), так и при передаче (по сети).

Системы контроля доступа: Обеспечивают аутентификацию (подтверждение личности), авторизацию (определение прав) и учет действий пользователей.

SIEM-системы (Security Information and Event Management): агрегируют и анализируют данные с различных источников (журналы, логи) для выявления аномалий и сложных атак в реальном времени.

2. Регламенты и процессы (Процедуры)
Технологии бесполезны без четких регламентов их использования. Ключевые процессы:

Управление уязвимостями: Регулярное сканирование, оценка и устранение уязвимостей в программном обеспечении и системах.

Реагирование на инциденты: Четкий план действий в случае кибератаки, определяющий роли, ответственность и этапы сдерживания угрозы, ликвидации последствий и восстановления работы.

Резервное копирование и восстановление: Регулярное и проверенное создание копий критически важных данных — главное оружие против ransomware.

Политика информационной безопасности: Внутренний документ, устанавливающий правила обработки информации, использования паролей, работы с электронной почтой и т.д.

3. Человеческий фактор (Обучение и культура) Самый сложный, но и самый важный элемент системы.

Регулярное обучение и повышение осведомленности: Сотрудники должны уметь распознавать фишинговые письма, знать правила создания надежных паролей и понимать последствия нарушения политик безопасности.

Формирование культуры безопасности: Безопасность должна стать неотъемлемой частью корпоративной культуры, а не восприниматься как обуза, навязанная IT-отделом.

Проведение учений: Тестовые фишинговые рассылки и моделирование инцидентов помогают оценить готовность сотрудников и отточить навыки команды реагирования.

Часть 3: Будущее информационной безопасности: тренды и прогнозы

Информационная безопасность — это «гонка вооружений», и ее будущее определяют несколько ключевых трендов.

Искусственный интеллект и машинное обучение. AI используется как защитниками для анализа огромных массивов данных и прогнозирования атак, так и злоумышленниками для создания самообучающихся вредоносных программ и автоматизации взлома.

Квантовые вычисления. Появление квантовых компьютеров создаст угрозу для современных алгоритмов шифрования, что потребует перехода на постквантовую криптографию.

Нормативное регулирование. Государства все активнее вмешиваются в цифровое пространство, принимая законы, подобные GDPR в Европе или ФЗ-152 в России. Комплаенс (соблюдение нормативных требований) становится драйвером инвестиций в ИБ.

Концепция «нулевого доверия» (Zero Trust). Классическая модель «замок и ров», где внутренняя сеть считается безопасной, устарела. Zero Trust предполагает принцип «никому не доверяй, проверяй все» — каждый запрос на доступ проверяется, независимо от его источника.

Безопасность цепочек поставок. Атаки, подобные SolarWinds, показали, что компрометация одного поставщика программного обеспечения может поставить под угрозу тысячи его клиентов. Безопасность всего жизненного цикла ПО становится критически важной.

Таким образом, информационная безопасность — это непрерывный и динамичный процесс, а не конечное состояние. В современном гиперсвязанном мире невозможно создать абсолютно неуязвимую систему. Однако построение сбалансированной защиты, основанной на глубоком понимании угроз, внедрении передовых технологий, отлаженных процессов и, что самое главное, на

постоянном обучении и повышении осведомленности людей, позволяет организациям значительно снизить риски и уверенно действовать в цифровой среде. Успех в этой области определяется способностью не только противостоять известным угрозам, но и адаптироваться к новым, еще неизведанным вызовам.

Список литературы:

1. Галатенко, В. А. Основы информационной безопасности [Текст]: учебное пособие для вузов / В. А. Галатенко; под ред. В. Б. Бетелина. — 4-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ); БИНОМ. Лаборатория знаний, 2015. — 205 с.

2. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]: учебное пособие для вузов / А. А. Малюк, В. И. Панасенко. — 2-е изд., стер. — Москва: Горячая линия–Телеком, 2016. — 334 с.: ил.

3. Что такое информационная безопасность? [Электронный ресурс] // URL: [https://mws.ru/blog/chto-takoe-informacionnaya-bezopasnost/] (дата обращения: 14.11.2025).

4. Обзор рынка информационной безопасности России 2025 [Электронный ресурс] //URL: [https://www.cnews.ru/reviews/informatsionnaya_bezopasnost_2025] (дата обращения 15.11.2025).

5. Что такое информационная безопасность? [Электронный ресурс] // URL: [https://fin-ctrl.ru/glossary/informacionnaya-bezopasnost] (дата обращения: 15.11.2025).