СЕКЦИЯ 3. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056

Аскарова Г.Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. Статья посвящена анализу современных технологий защиты информации в условиях стремительного роста цифровизации и киберугроз. Рассматриваются причины уязвимости информационных систем, классификация методов защиты и перспективы внедрения интеллектуальных систем. Обоснована необходимость комплексного подхода, включающего правовую донастройку, обучение и интеграцию ИИ-технологий для эффективного управления информационной безопасностью.

Ключевые слова: информационная безопасность, киберугрозы, методы защиты, искусственный интеллект, правовое регулирование.

Открыть сегодня новостную ленту – и почти сразу наткнуться на очередной заголовок о масштабной утечке данных: от электронной почты госслужащих до всей переписки пользователей в мессенджерах. Что пугает больше всего – не масштаб потерь, а то, как рутинно воспринимаются такие события. В условиях, когда темпы цифровизации превосходят способность общества и государства выстроить устойчивую систему информационной безопасности, любая структура оказывается под угрозой. Уязвимость – это не аномалия, а новое «нормальное» состояние.

За последние три года, по данным Минцифры РФ, число инцидентов ИБ в критической инфраструктуре увеличилось на 48 %. Причем наибольшая доля пришлась на так называемые «человеческие» сбои – компрометация учетных данных, несанкционированный доступ через устаревшее ПО, ошибки в конфигурации систем [1]. Это подтверждают и наблюдения Мирсаидовой Н. С., которая подчеркивает: ключевые угрозы проистекают не только из-за внешнего вмешательства, но и из-за плохо настроенной архитектуры защиты самой системы [1].

Особо уязвимым слоем стали персональные данные – сырье для черного рынка и оружие в руках злоумышленников. Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006 г. хоть и декларирует защиту прав субъекта, но, по факту, практически не адаптирован к реалиям алгоритмического сбора и трансграничной передачи данных. Особенно это

заметно в контексте социальных сетей, где пользователь, соглашаясь с пользовательским соглашением, открывает доступ к своим предпочтениям, биометрии, геолокации, списку контактов. Как замечает Кириченко А.В., соцсети – это не просто площадки для общения, это настоящие платформы слежки, где безопасность сводится к «доверяй, но проверяй» [2].

Рынок, конечно, реагирует: появляются новые стандарты, решения, попытки регулирования. Однако пока технологическая и правовая базы развиваются с разной скоростью, уязвимость остается встроенной функцией цифровой среды. Это и есть та самая точка бифуркации, когда либо будут предприняты системные усилия по обновлению подходов, либо мы продолжим латать дыры на корабле, плывущем по штормящему морю данных.

Если упростить всю экосистему защиты информации до трех составляющих – технология, человек, регламент – то провалы случаются на каждом уровне. В техническом плане существует солидный арсенал: криптография, двухфакторная аутентификация, шифрование дисков, межсетевые экраны, антиспам-фильтры, DLP-системы, honeypot-ловушки и многое другое. Но какие из этих решений действительно работают?

Абдыраева Н.Р. классифицирует методы защиты по четырем направлениям: физические, аппаратные, программные и организационные [5]. Каждое из направлений имеет свою нишу. К примеру, аппаратные методы – это защита информации на уровне процессоров, линий связи, источников питания. Они почти не уязвимы для вирусов, но неэффективны против социальной инженерии. Программные методы включают антивирусы, фаерволы и операционные системы с встроенной политикой безопасности. Однако они уязвимы при наличии доступа администратора. Организационные меры – как ни странно – оказываются самыми слабыми: по данным Positive Technologies за 2023 г., в 76 % случаев причиной инцидентов становится именно игнорирование или отсутствие регламентов поведения с информацией.

Жидко Е.А. подчеркивает: одна из главных проблем в РФ – отсутствие продуманной информационной политики внутри организаций, особенно в малом и среднем бизнесе. Без нее все технические меры становятся декоративными [3]. Даже такие простые действия, как смена паролей раз в 90 дней или ограничение прав доступа по принципу необходимости, часто игнорируются.

Среди современных технологий на особом месте стоят системы биометрической идентификации и аутентификации [4]. Мирсаидова Н.С. подробно анализирует плюсы и минусы биометрических решений: с одной стороны, это высокая точность идентификации, с другой – почти полная невозможность «сменить» данные при утечке [1]. Кто-то может сменить пароль, но не сетчатку глаза.

Еще одна растущая область – шифрование. От шифра Цезаря до алгоритмов AES и RSA – прогресс очевиден. Но, как показал случай с

атакой на ColonialPipeline в США (май 2021 г.), наличие шифрования не спасает, если скомпрометирован ключ. Поэтому ключевое внимание в новых реалиях уделяется управлению ключами и их безопасному распределению.

Таким образом, эффективность технологии – это не только качество алгоритма, но и то, как она встроена в человеческий и регламентный контекст. Иначе – это бронежилет без солдата.

Применение искусственного интеллекта и поведенческой аналитики в защите информации – не из области фантастики. Уже сейчас в корпоративных системах начинают внедряться нейросетевые алгоритмы, способные распознавать аномалии в действиях пользователей, выявлять подозрительные паттерны доступа, прогнозировать потенциальные инциденты. Такие системы, как SIEM и UEBA, работают по принципу: «пользователь никогда не заходил в систему ночью – значит, сейчас есть риск компрометации». Это качественно новый уровень.

Сидлер М.О. акцентирует внимание на необходимости перехода от реактивных к проактивным мерам безопасности – и именно в этом направлении движутся интеллектуальные технологии [5]. Они не просто блокируют угрозы – они умеют учиться, адаптироваться, предугадывать.

Но вместе с этим появляются и новые вызовы. Например, насколько допустимо использовать поведенческий анализ без ведома самого пользователя? Где проходит граница между необходимой защитой и нарушением приватности? Законодательство пока не успевает реагировать. И если в ЕС действует GDPR с четкими принципами обработки данных, то в России регулирование фрагментарно и неполно. Закон № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» содержит положения о защите, но не покрывает тонкости использования ИИ-систем в этой сфере [2].

При этом уровень угроз продолжает расти. Классический фишинг уже давно дополняется схемами социальной инженерии, а с развитием deepfake-технологий можно сгенерировать даже видеообращение «от начальника», просящее переслать конфиденциальный отчет. Кириченко А.В. подчеркивает: цифровая идентичность становится все менее защищенной, а уязвимости – все более психологическими [2].

Вывод здесь не в апокалипсисе, а в необходимости комплексного подхода. Без правовой донастройки, без образовательных программ, без усиления технологической суверенности говорить о надежной информационной защите – самообман. Сегодня надо не просто внедрять решения, а переосмыслять саму архитектуру цифровой безопасности. Потому что главная технология защиты информации – это мышление: системное, критическое и предвосхищающее.

Список использованных источников:

1. Мирсаидова Н.С. Основы информационной безопасности // Государственное управление. 2022. № 2 (56). С. 314–321.
2. Кириченко А.В. Защита информации в социальных сетях // Юридическая наука: история и современность. 2022. № 10. С. 78–83.
3. Жидко Е.А., Макаров Д.О., Небабин С.А. Защита информации с использованием информационных технологий // Информационные технологии в строительных, социальных и экономических системах. 2022. № 3 (29). С. 30–33.
4. Исмагилова А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. 2024. № 1 (109). С. 178–188.
5. Абдыраева Н.Р., Турсунбаев Ф.С., Жумабай Уулу Н. Современные способы и средства защиты информации // Бюллетень науки и практики. 2022. Т. 8, № 4. С. 426–431.

Askarova G.F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

INFORMATION PROTECTION TECHNOLOGIES

Abstract. The article examines modern technologies for information protection in the context of rapid digitalization and increasing cyber threats. It analyzes the causes of system vulnerabilities, classification of protection methods, and prospects for integrating intelligent systems. The paper highlights the need for a comprehensive approach, including legal adaptation, education, and implementation of AI technologies to ensure effective information security management.

Keywords: information security, cyber threats, protection methods, artificial intelligence, legal regulation.