УДК 004.056.5

АНАЛИЗ УЯЗВИМОСТЕЙ И УГРОЗ В КОРПОРАТИВНЫХ СЕТЯХ

А.В. Шмавгонец

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Рассматриваются актуальные вопросы анализа уязвимостей и угроз информационной безопасности в корпоративных сетях. Особое внимание уделяется защите баз данных как ключевому элементу корпоративных информационных систем. Приведен анализ статистических данных по киберпреступности в Республике Беларусь за 2025 год, включая динамику финансовых потерь и структуру правонарушений. Обоснована необходимость регулярного проведения тестирования на проникновение (пентеста) как эффективного метода выявления недостатков защиты и прогнозирования экономических рисков.

Ключевые слова: информационная безопасность; корпоративная сеть; базы данных; уязвимости; угрозы; киберпреступность; тестирование на проникновение; пентест; анализ защищенности; экономические риски.

VULNERABILITY AND THREAT ANALYSIS IN CORPORATE NETWORKS

A.V. Shmavgonets

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. The current issues of analyzing vulnerabilities and threats to information security in corporate networks are considered. Special attention is paid to database protection as a key element of corporate information systems. The analysis of statistical data on cybercrime in the

Republic of Belarus for 2025, including the dynamics of financial losses and the structure of offenses, is presented. The necessity of regular penetration testing (pentest) is substantiated as an effective method of identifying protection deficiencies and forecasting economic risks.
Keywords: information security; corporate network; databases; vulnerabilities; threats; cybercrime; penetration testing; pentest; security analysis; economic risks.

Введение

В современном мире информационные технологии играют ключевую роль в деятельности организаций и предприятий. Одним из важнейших компонентов корпоративных информационных систем являются базы данных, в которых аккумулируются сведения о клиентах, сотрудниках, финансовых операциях, партнерах, а также критически важная коммерческая информация.

Необходимость защиты информации в базах данных обусловлена также тем, что современные корпоративные системы тесно интегрированы с внешними сервисами, облачными решениями и сетевыми приложениями. Это значительно расширяет поверхность атаки и повышает вероятность компрометации данных.

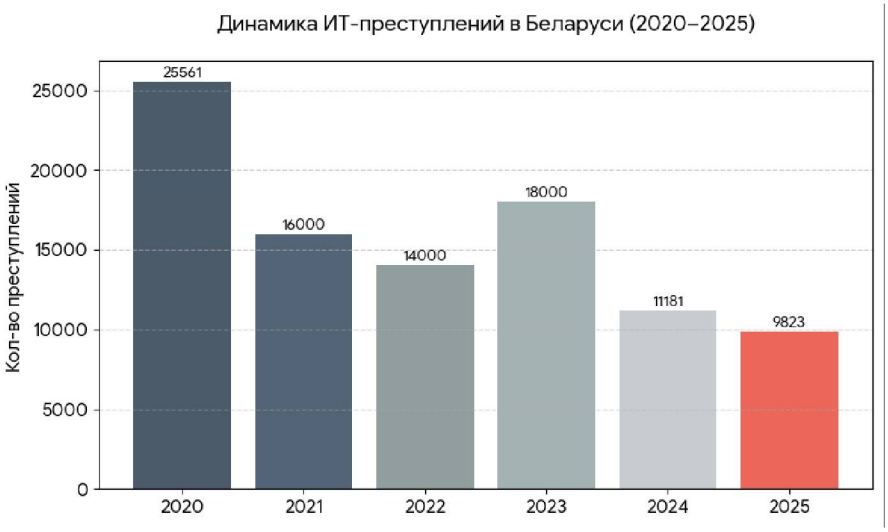
Актуальность темы определяется тем, что обеспечение информационной безопасности корпоративных баз данных является ключевым условием стабильной работы предприятия, непрерывности бизнеспроцессов и доверия клиентов.

Основная часть

На начальном этапе развития сетевых технологий ущерб от вирусных и других типов компьютерных атак был невелик, так как зависимость мировой экономики от информационных технологий была мала. В настоящее время в условиях значительной зависимости бизнеса от электронных средств доступа и обмена информацией и постоянно растущего числа атак ущерб от самых незначительных атак, приводящих к потерям машинного времени, исчисляется миллионами долларов, а совокупный годовой ущерб мировой экономике составляет десятки миллиардов долларов.

Статистические итоги 2025 года в Республике Беларусь демонстрируют тревожные тенденции. Зарегистрировано снижение количества киберпреступлений на 6% (9 823 преступления), однако при этом наблюдается рост «качества» атак: финансовые потери граждан составили более 54 миллионов белорусских рублей. От действий преступников пострадали 19 тысяч человек, при этом около 96% всех киберпреступлений направлены на завладение денежными средствами. Средний чек кражи вырос с 2 500 BYN в 2024 году до 4 000+ BYN в 2025-м, участились случаи хищения сумм свыше 100–150 тысяч рублей.

Правоохранительными органами было выявлено и заблокировано почти 15 тысяч мошеннических интернет-ресурсов.



Статистические итоги 2025 года

Информация, обрабатываемая в корпоративных сетях, является особенно уязвимой, чему способствуют увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации, сосредоточение в базах данных информации различного уровня важности и конфиденциальности, расширение доступа круга пользователей к информации, хранящейся в базах данных, и к ресурсам вычислительной сети, увеличение числа удаленных рабочих мест, широкое использование глобальной сети Internet и различных каналов связи, автоматизация обмена информацией между компьютерами пользователей.

Корпоративная информационная система представляет собой сложную структуру, в которой объединены различные сервисы, необходимые для функционирования компании. Эта структура постоянно меняется – появляются новые элементы, изменяется конфигурация существующих. По мере роста системы обеспечение информационной безопасности и защита критически важных для бизнеса ресурсов становятся все более сложной задачей.

Для того чтобы выявить недостатки защиты различных компонентов и определить потенциальные векторы атак на информационные ресурсы, проводится анализ защищенности. Эффективный способ анализа – тестирование на проникновение (пентест), в ходе которого моделируется реальная атака злоумышленников. Цель тестирования – обнаружить возможные уязвимости и недостатки, способные привести к нарушению конфиденциальности, целостности и доступности информации, спровоцировать некорректную работу системы или привести к отказу от обслуживания, а также спрогнозировать возможные финансовые потери и экономические риски.

Технологии информационной безопасности очень быстро устаревают, решение, оптимальное для предприятия заказчика на данный момент, не будет таковым через некоторое время. Поэтому многие специалисты по информационной безопасности рекомендуют проводить penetration test на регулярной основе, наилучшее решение – ежегодно.

Заключение

В результате проведенного анализа установлено, что корпоративные сети и базы данных в современных условиях подвергаются качественно новым угрозам. Интеграция с внешними сервисами расширяет поверхность атаки, делая традиционные методы защиты недостаточными. Статистика киберпреступлений в Беларуси за 2025 год подтверждает общемировой тренд: снижение количества атак сопровождается резким ростом их эффективности и финансовых потерь для жертв (средний чек превысил 4 000 BYN). Это свидетельствует о профессионализации киберпреступности и ее нацеленности на непосредственное хищение средств.

В сложившихся условиях ключевым инструментом обеспечения информационной безопасности становится регулярное тестирование на проникновение. Ежегодное проведение таких работ должно стать обязательной практикой для предприятий, стремящихся к сохранению непрерывности бизнес-процессов и защите критически важных данных.

Список использованных источников

1. Олифер В.Г., Олифер Н.А. (2007) Компьютерные сети. 2-ое изд. Москва, Вильямс.

2. Коллинз М. (2019) Защита сетей. Подход на основе анализа данных. Москва, ДМК.

3. Следственный комитет Республики Беларусь (2026) Официальные данные о состоянии киберпреступности в Республике Беларусь за 2025 год

4. Министерство внутренних дел Республики Беларусь (2026) Анализ финансовых потерь граждан от кибермошенников в 2024-2025 г.

References

1. Olifer V.G., Olifer N.A. (2007) Computer Networks. 2nd ed. Moscow, Williams Publishing House (in Russian).

2. Collins M. (2019) Network Security Through Data Analysis. Moscow, DMK Press (in Russian).

3. Investigative Committee of the Republic of Belarus (2026) Official Data on the State of Cybercrime in the Republic of Belarus for 2025 (in Russian).

4. Ministry of Internal Affairs of the Republic of Belarus (2026) Analysis of Citizens' Financial Losses from Cyber Fraud in 2024-2025 (in Russian).

Сведения об авторах

Шмавгонец А.В., магистрант факультета информационная безопасность. Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nastamoom2018@gmail.com

Information about the author

Shmavgonets A.V., Master's Degree Student, Faculty of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", nastamoom2018@gmail.com