Амелютин Е.В., Решетников Д.Д. Актуальность проблемы внутренних угроз в информационных системах // Международный журнал информационных технологий и энергоэффективности. – 2024. –
Т. 9 № 3(41) с. 38–48

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ВНУТРЕННИХ УГРОЗ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

[1] Амелютин Е.В., [2] Решетников Д.Д.
ФГБУО ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: [1] amelyutin9@yandex.ru , [2] r.daniil1@outlook.com

В статье был проведён анализ предметной области, определены характеристики внутренних угроз в информационных системах. Перечислены методы анализа сетевого трафика.

Ключевые слова: Информационные системы, внутренние угрозы, информационная безопасность.

THE RELEVANCE OF THE PROBLEM OF INTERNAL THREATS IN INFORMATION SYSTEMS

[1] Amelyutin E.V., [2] Reshetnikov D.D.
MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: [1] amelyutin9@yandex.ru , [2] r.daniil1@outlook.com

The article analyzed the subject area and identified the characteristics of internal threats in information systems. Methods for analyzing network traffic are listed.

Keywords: Information systems, internal threats, information security.

В настоящее время информационные системы (далее ИС) используются в организациях для хранения, обработки и дальнейшего использования данных. Что будет считаться ценными сведениями зависит от компании, это может быть стратегическая информация, дающая преимущество перед конкурентами.

Известно, что человек играет важную роль в вопросах информационной безопасности (далее – ИБ), поэтому эта особенность должна приниматься во внимание наряду с технологическими аспектами. Эффективное управление ИБ невозможно реализовать без учета ролей пользователей и организаций. Например, атаки, исходящие от инсайдеров, могут иметь серьезные последствия для надлежащего функционирования компьютерных систем. Существует множество типов инсайдеров: аудиторы, клиенты, постоянные или временные сотрудники, бывшие сотрудники и поставщики. Многие из них имеют законную возможность доступа к одной или нескольким системам, например, с помощью механизма аутентификации. Инсайдеру не нужно тратить столько сил и времени на доступ к целевой информации, как

внешним злоумышленникам. К тому же, организации часто им доверяют, благодаря чему снижается риск их идентификации и повышается реализация угрозы.

Инсайдерские угрозы нарушают конфиденциальность, целостность и доступность информации. Удаление, модификация, а также раскрытие важной информации являются примерами реализации угроз, мотивация которым может послужить коррупция, шпионаж, растрата, вымогательство, невежество и саботаж [4].

Область инсайдерских угроз ИБ в организациях сосредоточена главным образом на отношениях, намерениях и поведении сотрудников. Удобство совершения инцидента и наличие мотива для этого играют важную роль в этиологии преступного поведения сотрудников.

Поэтому информационные системы подвергаются различным угрозам, приходящим извне и изнутри. Действия злоумышленников могут повлечь риски нарушения информационной безопасности компании ИБ, путём использования уязвимости в информационных системах мерах информационной безопасности ИБ. Меры вводятся организациями с целью снижения вероятности реализации угрозы для обеспечения безопасности информации, которая считается для них наиболее ценной.

Одним из возможных решений проблемы обнаружения внутренних угроз и мониторинга поведения пользователей является использование программного обеспечения для мониторинга сетевого трафика. Его основная задача – анализ сетевого трафика и его возможной блокировки при выявлении аномалий.

Представленный подход тесно связан с понятием SOC (Security Operations Center - центр мониторинга информационной безопасности) и его региональной адаптацией сети.

SOC – это организационное и техническое решение, которое охватывает [5]:

1. Людей, их организацию – структура управления, знания и навыки, необходимые для работы и обучения SOC;
2. Процессы – сосредоточение внимания на мониторинге безопасности, управлении инцидентами безопасности, идентификацией угроз, цифровой криминалистике и управлению рисками, управлению уязвимостями, анализом безопасности и т. д.;
3. Технологии – решения для мониторинга безопасности, готовность к сетевой инфраструктуре, сборы событий, анализ и контроль безопасности, управление журналами, отслеживание и оценка уязвимостей, коммуникация, коммуникация и т. д.

Ключевым процессом SOC является управление инцидентами информационной безопасности. Как правило, команда SOC контролирует индикаторы компрометации защищенных активов, обнаруживает события безопасности, классифицирует некоторые из них как инциденты и обеспечивает правильную реакцию на инциденты.

Сбор и анализ данных об инцидентах ИБ является ключевым действием SOC. Сбор данных связан с мониторингом IT-инфраструктуры, активов и процессов, принадлежащих организации. SOC собирает данные из разных источников имеющих, в свою очередь, разные форматы. При этом процесс сбора синхронизируется со временем. Количество собранных данных должно быть необходимым и достаточным для вывода инцидентов или их предпосылок.

Обычно рассматриваются следующие источники данных для регистрации сообщений:

- Оборудование, связанное с безопасностью, такое как брандмауэры, системы обнаружения/предотвращения вторжений (IDS/IPS), веб-прокси, системы обнаружения вредоносных программ;
- Компоненты сетевой инфраструктуры, например маршрутизаторы, коммутаторы, точки доступа, шлюзы;
- Операционные системы, платформы виртуализации, базы данных, сетевые приложения;
- Компоненты физической безопасности и другие (параметры сетевого потока, сетевые пакеты; файлы, особенно файлы конфигурации, значения хэш, файлы HTML и т. д.).

Помимо SOC существуют системы мониторинга и аудита. Они представляют собой эффективное средство для проведения расследований инцидентов. Современные системы аудита умеют фиксировать практически все действия пользователей. Однако эти системы не способны предотвратить утечку информации, так как для этого необходима система реагирования на события и принятия решений (SIEM - Security Information and Event Management), которая может определить, какие действия представляют угрозу. Если реакция на нарушение не будет немедленной, последствия инцидента могут стать неизбежными.

Системы защиты конфиденциальных данных от внутренних угроз, также известные как системы предотвращения утечек данных (DLP - Data Leak Prevention), контролируют потоки утечки данных в режиме реального времени. Они могут быть комплексными, охватывающими множество потенциальных каналов для утечки, или точечными, фокусирующимися на определенных путях потенциальной утечки. Эти системы используют превентивные технологии, которые не только регистрируют нарушения информационной безопасности, но и предотвращают возможные утечки информации. Качество такого контроля напрямую зависит от способности системы идентифицировать конфиденциальную информацию, что обеспечивается алгоритмами контентной (анализ содержимого трафика) или контекстной (анализ метаданных трафика) фильтрации. Большинство современных систем DLP также имеют функции шифрования данных (такие системы также известны как системы защиты и контроля информации, IPC). Они также могут использовать защищенные хранилища данных, такие как криптоконтейнеры, которые учитывают не только ключ шифрования, но и различные факторы, такие как уровень доступа пользователя. Дополнительно системы DLP могут проводить анализ поведения пользователей, вносящий свои особенности, и иметь различные дополнительные функции [13].

Термин DLP стал широко известен в бизнес среде в начале 2000-х, когда компания Symantec первой сформулировала эту концепцию. Ранее информационная безопасность компаний сосредоточивалась на защите от внешних угроз, таких как DDoS-атаки, вирусы и взломы, с использованием антивирусов и систем обнаружения вторжений. Однако Symantec обратила внимание на новую угрозу – внутренних нарушителей и инсайдеров, и предложила идею, что исходящий трафик также может представлять угрозу компании и должен быть контролируем.

Согласно концепции Symantec, весь исходящий трафик должен обязательно проходить через систему DLP, которая автоматически проверяет его на соответствие установленным

политикам безопасности. В случае обнаружения нарушения система DLP может либо заблокировать трафик, либо уведомить службу информационной безопасности об инциденте.

Внутренние угрозы информационной безопасности являются более опасными, чем внешние. Это показано на Рисунке 1, где 68% – низкая защищенность от внешних угроз, а 96% от внутренних [9]:

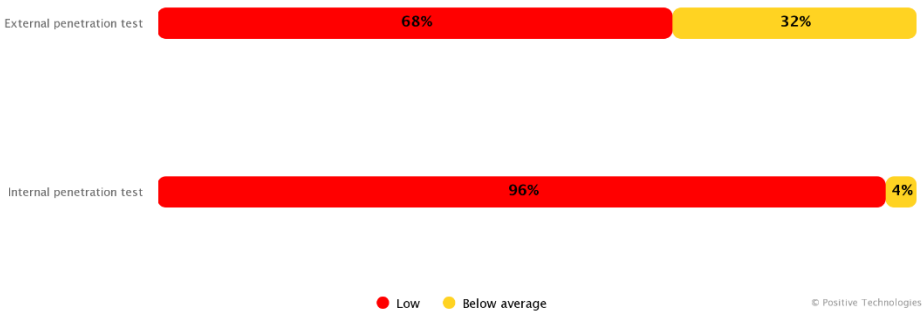

Рисунок 1 – Уровень безопасности организаций в 2022 году

Возникновению внутренних угроз могут послужить ошибки сотрудников, бездействие, халатность. Из-за этих действий компании получают серьёзный ущерб, как материальный, так и репутационный. Для уменьшения возникновения вероятности возникновения инцидентов необходимо проводить различные мероприятия: организационные, правовые и технические.

Организационные методы защиты информации направлены на установление правил доступа к информации в компьютерных системах с целью предотвращения возможных угроз безопасности [11]. Среди наиболее эффективных организационно-административных методов защиты информации можно выделить:

1. разрешение доступа к защищенной информации только ~~у~~авторизованным сотрудникам;
2. хранение носителей информации в местах, недоступных для посторонних лиц;
3. ограничение доступа к информационным ресурсам в соответствии с должностными обязанностями и функциями сотрудников.

Защита информации с точки зрения правовых аспектов осуществляется через действующее законодательство и нормативные акты, которые определяют правила и стандарты для обеспечения безопасности информации. Обеспечение информационной безопасности входит в область национальной безопасности и регулируется законодательно через Конституцию РФ, законы в области безопасности, конституции и нормативными актами субъектов, а также международными договорами и соглашениями.

Кроме программных продуктов, таких как DLP-системы, технические средства и меры обеспечения информационной безопасности включают в себя другие инструменты, доступные для компании. Ими могут быть криптографические средства защиты, а также средства, необходимые для распознавания сотрудников. С технической точки зрения меры защиты информации должны опираться на модель построения ИС предприятия, которая позволяет обеспечить защиту от утечек конфиденциальной информации [12].

Исходя из этого, внутренними нарушителями могут стать лица, находящиеся в компании и имеющие доступ к данным. Их действия зависят от имеющихся в зоне доступа ограничений, устанавливаемых организационно-техническими мерами. Ключевым фактором для таких нарушителей является их уровень доступа к информации и должность внутри организации, поскольку доступ к данным и их использование определяются существующими политиками безопасности и системой ролей сотрудников.

Большинство внутренних угроз компании представлены тремя категориями людей:

1. Сотрудники, которые испытывают негативные эмоции к компании или недовольны своим положением. Их действия могут быть мотивированы личными обидами, желанием мести. Возникновение таких ситуаций может быть обусловлено выговором, конфликтом с руководством или отменой премии;
2. Сотрудники, стремящиеся получить легкие деньги. Они могут пытаться использовать свое положение в компании для личных целей, например, продавать информацию конкурентам, использовать личные данные клиентов или привлекать клиентов к своей стороне;
3. Внедренные агенты. Это сотрудники, которые были завербованы конкурентами для сбора и передачи важной информации, проведения провокаций, переманивания других сотрудников, а также нанесения ущерба организации. Часто это высокопоставленные сотрудники или те, кто имеет привилегированный доступ к информации.

Внутренние угрозы информационной безопасности классифицируют по следующим признакам:

1. Обход защитных мер и ограничений доступа, который заключается в использовании дополнительных технических средств и программного обеспечения, скрывающих действия злоумышленника. Эти программы могут включать в себя шифрование данных, глубокую архивацию, преобразование файлов и использование различных языков кодирования. Такие меры усложняют выявление нарушителя и определение его незаконной деятельности, что позволяет ему оставаться незамеченным на протяжении длительного времени;
2. Раскрытие конфиденциальной информации, включающее копирование документов, передачу данных через интернет конкурентам или заинтересованным лицам, а также перенос на сменные носители информации. Обычно это затрагивает определенные категории информации, такие как коммерческая тайна или личные данные клиентов компании. Иногда разглашение конфиденциальной информации происходит случайно, без злого умысла;
3. Кража информации - нарушение информационной безопасности, которое целенаправленно направлено на получение закрытого доступа к сведениям повышенной важности, таким как государственные и коммерческие секреты, а также финансовая отчетность;
4. Нарушение конфиденциальности и авторских прав - использование информации, права на которую принадлежат только ее владельцу, например, семейные или интимные сведения, фотографии, видеоматериалы. Публикация такой информации в СМИ и открытых источниках в интернете требует согласия владельца.

С другой стороны, в течение многих лет исследования, посвященные информационной безопасности, указывают на человека в качестве основного виновника инцидентов, угрожающих информационной безопасности. Необходимо отметить, что 70% всех случаев

нарушения информационной безопасности в Польше в 2015 году были совершены сотрудниками организаций (из которых 48% текущие и 22% бывшие сотрудники) [3].

Люди являются самым слабым звеном в системе информационной безопасности в организациях. Действия, направленные на сотрудников и субподрядчиков, имеют решающее значение. Это подтверждается словами автора, который отмечает [14], что простых технических мер уже недостаточно для обеспечения информационной безопасности.

Приведенный выше тезис подтверждается глобальным исследованием информационной безопасности, проводимым EY (2017) [10], которое показывает, что более широкий пробел в мерах безопасности включает в себя отсутствие осведомленности сотрудников. Таким образом, разработка соответствующей модели поведения сотрудников в организации играет не меньшую роль в информационной безопасности организации, чем любые другие технические меры.

Чтобы понять суть неэтичного поведения в области безопасности, важно определить, что является таким поведением, и разработать инструменты для его измерения. Для этого были выявлены различные типы поведения, связанного с безопасностью со стороны сотрудников [6], включая злоупотребление компьютером, неправильное использование информационных систем, не связанные с работой действия и нарушение информационной безопасности. Эти исследования дают дополнительное понимание «плохого» поведения, связанного с безопасностью. Однако большинство этих исследований не определяли такое поведение и не разработали инструменты для его оценки. Кроме того, таким поведением могут являться действия, связанные с такими серьезными нарушениями, как кража или повреждение данных на компьютере, несанкционированный доступ к данным компании и взлом компьютера. Основным направлением исследования являются часто встречающиеся действия, которые относительно легко наблюдать или контролировать на рабочем месте, что позволяет разработать короткие инструменты самоотчета, чтобы узнать больше об усилиях сотрудников для защиты информации.

Данные в каждой компании являются одним из наиболее важных активов; следовательно, защита этих данных должна иметь высший приоритет [1]. Хотя компании имеют средства измерения безопасности и программное обеспечение, такие как брандмауэры, применение которых полностью не гарантирует отсутствие утечек данных. Это происходит, когда конфиденциальные данные раскрываются несанкционированными сторонами, намеренно или нет. Утечка данных может вызвать серьезные угрозы для компании. Потеря конфиденциальных данных может серьезно повлиять на репутацию компании, клиенты и доверие сотрудников, конкурентное преимущество и в некоторых случаях привести к закрытию компании, или политическим кризисам, таким как утечки Wikileaks [2].

Организации имеют конфиденциальную информацию под их контролем, такую как финансовые и запатентованные данные, номера кредитных карт, медицинские карты или номера социального страхования. Чтобы помочь защитить эти конфиденциальные данные и снизить риск от чрезмерного обмена, им нужно использовать программное решение, которое ограничит пользователей от передачи конфиденциальных данных тем людям, у которых их не должно быть.

Рассмотрим категории приложений NTMA (Network Traffic Monitoring and Analysis - анализ и контроль сетевого трафика) [7]. Их основные задачи: сбор и анализ данных,

необходимых для управления трафиком и устранения неполадок, с целью прогнозирования сети и определения источника проблем. Существуют четыре категории, которые определены в соответствии с конечной целью приложения: прогнозирование трафика; классификация трафика; управление неисправностями; обеспечение безопасности сети.

Прогнозирование трафика состоит из оценки будущего статуса сетевых соединений. Он служит основой для инженерии трафика, помогая определить, например, оптимальную нагрузку на сеть с сохранением уровей QoS (Quality of Service - качество сервиса).

Прогноз трафика часто сталкивается с проблемой прогнозирования временных рядов. Для решения подобных задач используется используются как классические методы прогнозирования (методы ARIMA (Autoregressive Integrated Moving Average) или SARIMA (Seasonal-ARIMA)), так и машинное обучение (нейронные сети) [12].

Классификация трафика направлена на выявление служб, создающих трафик. Это важный шаг для управления и мониторинга сети. Операторам нужна информация об услугах, например, для понимания их требований и их влияния на общую производительность сети.

Классификация трафика хорошо работает, при просмотре информации о сетевых и транспортных протоколах. Например, интернет-сервисы распознаются, через номера портов TCP/UDP. Тем не менее, классификация трафика не является простой задачей. Во-первых, количество интернет-услуг велико и с каждым днём их число увеличивается. Во-вторых, услуги должны быть идентифицированы путем просмотра небольшой информации, наблюдаемой в сети. В-третьих, мало информации остается видимой в пакетах, поскольку основная доля интернет-сервисов работает под протоколами шифрования (например, TCP под HTTPS). Наконец, интернет-сервисы динамичны и постоянно обновляются.

Управление неисправностью – это набор задач для прогнозирования, обнаружения и изоляции неисправностей в сетях. Цель такого управления состоит в том, чтобы минимизировать время простоя. Управление неисправностями может быть упреждающим, например, когда аналитика предсказывает дефекты на основе измерений, чтобы избежать сбоев, например, когда трафик и системные журналы оцениваются, чтобы понять текущие проблемы. В любом случае ключевым шагом в управлении неисправностями является локализация основной причины проблем.

В крупных сетях неисправности могут повлиять на различные элементы: например, неисправный маршрутизатор может перегружать другие маршруты, создавая тем самым цепь ошибок в сети. Информация о сетевых элементах будет отражена в системных журналах, связанных с проблемой, а поведение сети может быть изменено в различных аспектах. Обнаружение неисправности часто достигается с помощью методов обнаружения аномалий, которые идентифицируют девиантное поведение в трафике или необычные события в системных журналах.

Многие приложения NTMA были предложены для повышения безопасности организации [15]. Наиболее распространенной задачей является обнаружение недостатков безопасности, вирусов и вредоносных программ, чтобы изолировать зараженные машины и принять контрмеры с целью минимизации ущерба. То есть, существует два основных подхода при поиске злонамеренной сетевой деятельности: на основе сигнатур атаки; на основе обнаружения аномалий.

Методы на основе сигнатур атаки основываются на определении фингерпринта (цифровой отпечаток устройства) для атак. Такое программное решение для мониторинга осматривает исходный трафик/журналы/события, ищет известные сообщения, обмениваемые вирусами, вредоносными программами или другими угрозами; или типичные модели связи атак – то есть, аналогичные методу классификации трафика по поведению. Методы, основанные на сигнатуре, эффективны для блокировки хорошо известных атак, которые неизменны или медленно меняются. Эти методы, однако, требуют, чтобы атаки были ранее известны.

Методы, основанные на обнаружении аномалий основаны на анализе поведения сети. В них нормальное поведение сети суммируется по результатам измерений. Затем трафик в реальном времени начинает отслеживаться, и оповещения запускаются, когда поведение сети начнёт отличаться от нормального поведения. Методы обнаружения аномалий помогают обнаружить ранее неизвестные угрозы (например, эксплойты нулевого дня).

Мониторинг активности пользователей обычно включает отслеживание следующих действий пользователя:

1. Просматриваемые сайты;
2. Используемое программное обеспечение;
3. Снимки экрана;
4. Перехват вводимых данных с клавиатуры (кейлоггер).

Программное обеспечение для мониторинга работников позволяет работодателям отслеживать использование компьютеров, включая написанные и полученные сообщения электронной почты, другие электронные связи, приложения, комбинации клавиш, историю просмотра Интернета, время входа в сеть/выключение, файлы, копируемые в диски USB и физическое местоположение удалённых работников.

Программное обеспечение для мониторинга удаленного работника может:

1. Отслеживать время проекта;
2. Следить за всеми видами деятельности сотрудников;
3. Ограничить использование программ, не связанных с работой;
4. Определить факторы, усиливающие и замедляющие производительность;
5. Повысить безопасность против злонамеренных атак и инсайдерских угроз.

Однако, несмотря на вышеперечисленные причины, необходимо учитывать конфиденциальность каждого сотрудника [8]:

1. Мониторинг за пределами организации должен быть запрещен; необходимо позволить сотрудникам получить доступ ко всей информации, собранной с помощью методов или методов мониторинга и рассмотреть их мнение о такой информации; ограничить продолжительность мониторинга каждый день предложенным (максимум 2 часа в день).

2. Сотрудники должны знать об устройствах, которые будут использоваться для их мониторинга, как будут использоваться данные, и когда именно они будут контролироваться; также они должны быть уведомлены, когда телефонный мониторинг проводится благодаря использованию конкретного тона, который можно услышать сотрудником.

3. Работодатели должны собирать только информацию, относящуюся к принятию критических решений; причём этого недостаточно, чтобы оправдать мониторинг путем

необходимости повышения производительности, но также работодатели должны иметь возможность продемонстрировать, как была достигнута цель благодаря мониторингу.

Выводы

Проведён анализ предметной области, определены характеристики внутренних угроз в информационных системах. Определено, что необходимость мониторинга действий пользователей обусловлена низкой осведомлённостью сотрудников компании в области ИБ. Это, в свою очередь, может повлечь за собой утечку конфиденциальных данных компании, несмотря на соблюдение технических мер защиты информации.

Определены методы анализа сетевого трафика, которые необходимо применять для его прогнозирования и классификации, управления неполадками в сети и обеспечения безопасности. Часть таких методов использует машинное обучение, статистику по предыдущим измерениям трафика и разбор пакетов трафика.

Одним из решений по защите информации в компании от внутренних угроз является использование ПО для мониторинга и прогнозирования сетевого трафика с применением отслеживания рабочих мест сотрудников.

Для разработки программы по прогнозированию сетевого трафика планируется применить язык программирования C++, фреймворком Qt и библиотекой mlpack. Кроссплатформенный фреймворк Qt позволит отобразить информацию по трафику и сотрудникам в пользовательском интерфейсе и информацию по сотрудникам для контроля над временем их работы и запущенными приложениями с соответствующими правами. Библиотека mlpack используется для создания нейронной сети с целью анализа собранной информации в реальном времени и последующего обучения.

При создании планируется использовать нейросеть на основе многослойного персептрона. Она позволит точно определить возможных злоумышленников по собранным данным. Нарушением может являться: использование внешних носителей, попытку входа в систему под другой учетной записью, установка программ, модификация файлов, использование программ, не связанных с рабочей деятельностью. Использование метода ARIMA для прогнозирования временных рядов, позволит заранее определить нагрузку на трафик и принять соответствующие меры в целях обеспечения безопасности.

Список литературы

1. Tahboub R., Saleh Y. Data Leakage/Loss Prevention Systems (DLP).
2. What is WikiLeaks – URL: https://wikileaks.org/What-is-WikiLeaks.html (дата обращения 18.11.2023)
3. Stefaniuk T. Training in shaping employee information security awareness //Entrepreneurship and Sustainability Issues. – 2020. – Т. 7. – №. 3. – С. 1832.
4. Safa N. S. et al. Motivation and opportunity based model to reduce information security insider threats in organisations //Journal of information security and applications. – 2018. – Т. 40. – С. 247-257.
5. Bialas A., Michalak M., Flisiuk B. Anomaly detection in network traffic security assurance //International Conference on Dependability and Complex Systems. – Cham : Springer International Publishing, 2019. – С. 46-56.

6. Chu A. M. Y., So M. K. P. Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective //Sustainability. – 2020. – Т. 12. – №. 8. – С. 3163.
7. D'Alconzo A. et al. A survey on big data for network traffic monitoring and analysis //IEEE Transactions on Network and Service Management. – 2019. – Т. 16. – №. 3. – С. 800-813.
8. Moussa M. Monitoring employee behavior through the use of technology and issues of employee privacy in America //Sage Open. – 2015. – Т. 5. – №. 2. – С. 2158244015580168.
9. Results of penetration tests in 2022 – URL: https://www.ptsecurity.com/ww-en/analytics/results-of-pentests-2022/ (дата обращения 20.11.2023)
10. EY 20th Global Information Security Survey 2017 – URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/health/ey-20-global-information-security-survey-2017.pdf (дата обращения 20.11.2023)
11. Ахматов М. М., Тарчоков Б. А. Правовые и организационные методы защиты информации в компьютерных системах //Журнал прикладных исследований. – 2021. – Т. 6. – №. 6. – С. 580-584.
12. ARIMA & SARIMA: Real-World Time Series Forecasting – URL: https://neptune.ai/blog/arima-sarima-real-world-time-series-forecasting-guide (дата обращения 25.11.2023)
13. Сулавко А. Е. Технологии защиты от внутренних угроз информационной безопасности //Вестник Сибирской государственной автомобильно-дорожной академии. – 2011. – №. 19. – С. 45-51.
14. Parsons K. et al. The human aspects of information security questionnaire (HAIS-Q): two further validation studies //Computers & Security. – 2017. – Т. 66. – С. 40-51.
15. Liao H. J. et al. Intrusion detection system: A comprehensive review //Journal of Network and Computer Applications. – 2013. – Т. 36. – №. 1. – С. 16-24.

References

1. Tahboub R., Saleh Y. Data Leakage/Loss Prevention Systems (DLP).
2. What is WikiLeaks – URL: https://wikileaks.org/What-is-WikiLeaks.html (accessed 11/18/2023)
3. Stefaniuk T. Training in shaping employee information security awareness //Entrepreneurship and Sustainability Issues. – 2020. – Vol. 7. – No. 3. – p. 1832.
4. Safa N. S. et al. Motivation and opportunity based model to reduce information security insider threats in organizations //Journal of information security and applications. – 2018. – Vol. 40. – pp. 247-257.
5. Bialas A., Michalak M., Flisiuk B. Anomaly detection in network traffic security assurance //International Conference on Dependability and Complex Systems. – Cham : Springer International Publishing, 2019. – pp. 46-56.
6. Chu A.M. Y., So M. K. P. Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective //Sustainability. – 2020. – Vol. 12. – No. 8. – p. 3163.
7. D'Alconzo A. et al. A survey on big data for network traffic monitoring and analysis //IEEE Transactions on Network and Service Management. – 2019. – Vol. 16. – No. 3. – pp. 800-813.

8. Moussa M. Monitoring employee behavior through the use of technology and issues of employee privacy in America //Sage Open. – 2015. – Vol. 5. – No. 2. – pp. 2158244015580168.
9. Results of penetration tests in 2022 – URL: https://www.ptsecurity.com/ww-en/analytics/results-of-pentests-2022 / (accessed 11/20/2023)
10. EY 20th Global Information Security Survey 2017 – URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/health/ey-20-global-information-security-survey-2017.pdf (accessed 11/20/2023)
11. Akhmatov M. M., Tarchokov B. A. Legal and organizational methods of information protection in computer systems //Journal of Applied Research. – 2021. – Vol. 6. – No. 6. – pp. 580-584.
12. ARIMA & SARIMA: Real-World Time Series Forecasting – URL: https://neptune.ai/blog/arima-sarima-real-world-time-series-forecasting-guide (accessed 11/25/2023)
13. Sulavko A. E. Technologies of protection against internal threats to information security //Bulletin of the Siberian State Automobile and Road Academy. - 2011. – no. 19. – pp. 45-51.
14. Parsons K. et al. The human aspects of information security questionnaire (HAIS-Q): two further validation studies //Computers & Security. – 2017. – Vol. 66. – pp. 40-51.
15. Liao H. J. et al. Intrusion detection system: A comprehensive review //Journal of Network and Computer Applications. – 2013. – vol. 36. – No. 1. – pp. 16-24.