Канивец Александр Валентинович

Магистрант

Направление: Информатика и вычислительная техника

Магистерская программа: Информационные системы

Обеспечение информационной безопасности организации

Аннотация. Выделено два ракурса рассмотрения информационной безопасности. С одной стороны, это специальная отрасль информационной безопасности и часть общей информации. С другой стороны, информационная безопасность независимо от отраслевой принадлежности является видом информации и частью информационного ресурса государства. Рассмотрена роль терминов в упорядочении информационной безопасности с учетом значимости проблем информационной безопасности. Отмечена необходимость отличать информационные термины от общих терминов, характеризующих конкретную область. Даны определения информационной безопасности, информационного ресурса.

Ключевые слова: информационная безопасность, информация, информационные ресурсы, информационные технологии, технологические инновации, обучение и подготовка специалистов, международное сотрудничество.

Цель написания данной статьи, сформировать у будущих специалистов и руководителей системные знания по проблеме обеспечения комплексной защиты информационных ресурсов и управлению информационными рисками, а также практические навыки безопасной работы в информационных системах. Поставленные задачи включают формирование представлений об управлении информационными рисками, изучение методов и средств комплексной защиты информации, формирование навыков анализа защищённости информационных систем и т.д. Рассмотрение понятия информационной безопасности, её общего смысла, а также отличий между кибербезопасностью и информационной

безопасностью. Указание на то, что информационная безопасность включает в себя инструменты и процессы, которые компании и системы применяют в качестве защиты информации. Принципы информационной безопасности, это указание на три ключевых принципа: конфиденциальность, целостность, доступность [2, с. 156]. Описание наиболее выраженных угроз: физическое искажение или уничтожение информации, возможность несанкционированной модификации, опасность получения информации лицами, для которых она не предназначена и т.д.

Некоторые актуальные угрозы в 2025 году:

Программы-вымогатели (Ransomware) – блокируют системы или данные до выплаты выкупа.

Целевые APT-атаки – длительные и скрытые кампании по хищению данных, часто нацелены на конкретных должностных лиц или компании.

Фишинг – персонализированные письма, продуманные сценарии обманов по телефону, дипфейки.

Утечки данных – ошибки сотрудников, незащищённые API, старые CMS.

Инсайдерские угрозы – риски, которые исходят от сотрудников, подрядчиков или партнёров, у которых есть легальный доступ к системам.

Атаки через цепочку поставок – злоумышленники компрометируют менее защищённого подрядчика или программное обеспечение, чтобы проникнуть в крупную цель.

Некоторые тренды в кибербезопасности в 2025 году:

Искусственный интеллект (ИИ) в защите от кибератак – системы анализируют миллионы параметров сетевого трафика и поведения пользователей, выявляют аномалии.

Концепция Zero Trust («нулевого доверия») – ни один пользователь или устройство не может считаться безопасным по умолчанию, доступ предоставляется на основе строгой аутентификации, авторизации и постоянного мониторинга.

Защита растущей экосистемы IoT-устройств – производители IoT-устройств постепенно встраивают механизмы безопасности на уровне прошивки, а IoT-

устройства изолируют в отдельных сегментах сети с ограниченным доступом к критическим системам.

Безопасность гибридных рабочих мест – например, технология SASE (Secure Access Service Edge), которая объединяет сетевые функции и функции безопасности в единое облачное решение.

Автоматизация реагирования на инциденты (SOAR) – системы позволяют автоматизировать обработку инцидентов, минимизировать человеческий фактор и ускорять реагирование на атаки.

С 1 сентября 2025 года вступили в силу ключевые поправки в федеральном законодательстве о безопасности критической информационной инфраструктуры (КИИ). Некоторые изменения:

Исключение ИП из числа субъектов КИИ – это уменьшает административную нагрузку в отношении малых субъектов.

Закрепление требований к применяемому ПО, включая переход на программные продукты, входящие в российский реестр.

Введение ограничений иностранного участия – Федеральный закон №325-ФЗ, опубликованный 31 июля 2025 года, усиливает требования к отсутствию иностранного участия в субъектах КИИ и закрепляет ответственность за несоответствие этому требованию.

В 2025 году киберкоманды по-прежнему недоукомплектованы – 55% организаций считают свои киберкоманды недоукомплектованными. Особенно остро нехватка специалистов ощущается в компаниях с численностью от 500 до 5000 сотрудников.

Некоторые меры по решению проблемы:

Расширение образовательных программ по ИБ, например, программы, привязанные к конкретным ролям и задачам в сфере ИБ.

Более активное участие бизнеса в подготовке кадров, включая стажировки и практику на реальных предприятиях.

Создание собственных центров компетенций например, в области безопасной разработки программного обеспечения.

Использование онлайн-обучения, менторства и корпоративных тренингов – это помогает закрыть дефицит «мягких» навыков (критическое мышление, коммуникация и др.

Рост объемов информации, связанный с развитием практически любого современного бизнеса, увеличение количества пользователей информационной системы требуют внедрения надежного аппаратно-программного обеспечения, которое позволяет ликвидировать информационную разобщенность и наладить работу общедоступного информационного ресурса.

Решение этих и многих друих проблем заключается в развертывании мощных систем хранения данных. Они способны обеспечить своевременную обработку и надежное хранение постоянно возрастающего объема информации актуальных прикладных систем и сервисов с учетом растущих потребностей внедрения и развития корпоративных прикладных систем. Необходимо формирование единой среды управления информацией, в рамках которой происходит доступ и обработка данных.

Построение информационных систем управления это концептуальное решение комплекса задач интеграции существующих и перспективных ЛВС в единую информационную инфраструктуру с реализаций современных технологий распределенной обработки данных.

Обеспечение информационной безопасности в организации – это современный уровень защиты данных бизнеса и госсектора. Антагонистами этого процесса являются хакеры, фишинг, DDoS-атаки и многие другие совершенствующиеся сервисы. При отсутствии внедрения надежной системы информационной безопасности, организации привлекаются к административной или уголовной ответственности, что приводит к остановке бизнес-процессов, убыткам, потере репутации, судебным разбирательствам и другим неприятным последствиям. Целью обеспечения информационной безопасности (ИБ) в организации является создание условий, которые обеспечивают бесперебойную работу в условиях возможных атак. Защита информационной безопасности включает в себя меры по

обеспечению целостности и конфиденциальности, но при этом доступности для пользователей, имеющих необходимые права.

Рассмотрим этапы обеспечения информационной безопасности в организациях ПИК и ИНГОССТРАХ. Первое, это определение информации, которую необходимо защищать в организациях. На этом этапе требуется анализ информационных активов, например, базы данных, серверов, программного обеспечения.

Нужно распределить информацию по классификации критичности (от общего доступа до служебно-секретного (ДСП)). Важно, не забывать учитывать клиентские базы, облачные хранилища и т.д. Приотиризация рисков на соответствие требованиям стандарта Cloud Advisor, показал лучшие практики в областях безопасности, отказоустойчивости, анализирует облачную инфраструктуру с целью выявления комбинаций алертов, формирующих путь атаки, позволяя сфокусировать внимание на исправлении действительно важных рисков [4, с. 124]. Применялся в работе компании ПИК и ИНГОССТРАХ. Также, безагентный подход позволяет за минуты получить информацию о состоянии облака, обеспечивает 100% покрытие и не оказывает влияния на производительность виртуальных машин. Применение единой платформы Cloud Advisor CNAPP (Cloud Native Application Protection Platform) включает в себя CSRM (Cloud Security Posture Managemnt), CWPP (Cloud Workload Protection Platform) и KSPM (Kubernetes Security Posture Managemnt). Применение мульти-облако, в поддержке Yandex Cloud, Cloud.ru Advanced, VMware Cloud Director (Cloud.ru Enterprise, PTK, MWS, Selectel и др.), AWS, Azure, GCP и Huawei Cloud позволяет агрегировать всю информацию о мультиоблачной среде на единой панели отчетов.

Создан для бизнеса стандарт Cloud Advisor. В его платформу были добавлены сотрудники компаний ПИК и ИНГОССТРАХ с разными областями видимости и правами доступа. Таким образом, каждый из сотрудников имел доступ только к информации о своей части инфраструктуры. Также стандарт Cloud Advisor предоставляет мощное API получения информации о ресурсах и алертах. Он может

интегрировать продукт с SIEM, GRC, CMDB, системами постановки задач и мессенджерами для организации командной работы.

Реальный кейс. Организация передает по договору клиентскую базу на хранение облачному серверу и считает, что тем самым снимает с себя ответственность в случае утечки данных [3, с. 108]. Однако, прямую ответственность несет организация, а облачный сервер выступает, как провайдер. Соответственно именно организация обязана наладить информационную безопасность во всех своих направлениях. Важно регулярно проводить оценку программного обеспечения и аппаратных средств, используемых в организации. Таким образом, всегда есть данные о доступных ресурсах и их защищенности. В связи с этим, организация может прослеживать слабые места в системе безопасности и расставить приоритеты в обеспечении защиты информационной безопасности.

Далее проанализируем оценку возможных угроз. Угрозы безопасности информации – возможность возникновения такого явления или события, следствием, которого могут быть нежелательные воздействия на информацию. Информационные угрозы могут делиться на два вида, преднамеренные и случайные. Преднамеренные, это, например, хищение информации, компьютерные вирусы, физическое воздействие на технику. Случайные, это такие, как, ошибки пользователя, ошибки профессионалов, отказы и сбои аппаратуры, форс-мажорные обстоятельства.

Внутренние, неосторожность сотрудника организации и незнание в области информационной безопасности может привести к тому, что произойдет утечка данных. Технические сбои, сбой в работе оборудования. Организация обязана иметь план «Б» и в случае технических неполадок применить его, чтобы в работе организации не было сбоя, который мог бы привести, например, к потери данных.

Системы обнаружения и предотвращения атак – анализируют подозрительные активности в сети и могут автоматически реагировать на угрозы, блокируя вредоносные действия до того, как они смогут нанести ущерб; Антивирусные системы служат для предотвращения заражения вредоносным программным

обеспечением; Системы предотвращения утечек данных – защищают конфиденциальную информацию от утечек; Системы управления доступом и двухфакторная аутентификация минимизируют риски несанкционированного входа в системы.

Обязательно внедрение организационных мер, таких как, например, прохождение сотрудниками организации обучения в сфере информационной безопасности или повышения квалификации в этой области. По статистике, большое количество инцидентов информационной безопасности происходят по вине пользователей [5, с. 267]. Переход по фиштинговой ссылке, отправка персональных данных по незашифрованной почте, слабый пароль (12345) и т.д.

Важный вопрос разработки и внедрения документов по информационной безопасности, необходимых для организации. Для выстраивания работы по информационной безопасности наиболее важным этапом является разработка необходимых документов. Это важно не только для выстраивания архитектуры безопасности самой организации, но и для регулирования и закрепления ответственности ее сотрудников.

Пакет документов по информационной безопасности должен базироваться на действующем законодательстве, а именно: ФЗ от 27.07.2006 №152-ФЗ «О персональных данных», ФЗ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и т.д. За основу можно взять следующий перечень документов. Политика – является основным документом, в котором должно быть закреплено следующее:

1. Технические процессы обработки защищаемой информации в информационных системах;

2. Правила и процедуры идентификации и аутентификации пользователей информационных систем, политика разграничения доступа к ресурсам информационных систем, управления информационными потоками, управления инсталляцией компонентов программного обеспечения, контроля установки обновлений программного обеспечения и т.д. В документе в качестве объектов защиты рассматривается совокупность информационных ресурсов, средств и систем

обработки информации, используемых в соответствии с заданной информационной технологией, средства обеспечения функционирования информационных систем. Это требования к Техническим паспортам, иным документам.

Рассмотрим вероятные виды инцидентов в информационной безопасности. Инцидент информационной безопасности в организации – случай или событие, которое указывает на то, что информация организации украдена в связи с тем, что система защиты не сработали. Инциденты влекут нарушение работы организации. Они могут повлечь серьезные события, например, DDoS-атаку, кибератака, целью, которой является сделать веб-ресурс или сервис недоступным для пользователей путем перегрузки его огромным количеством трафика или запросов. Незаконный доступ к системам и данным. Фишинговая атака, например, электронные письма на почте для распространения вредоносных ссылок и вложений, которые могут выполнять различные функции; Вредоносное программное обеспечение, вирусы, рекламное программное обеспечение и т.д. DoS-атака ведет к серьезным последствиям.

Ошибки сотрудников организации, человеческий фактор. Нажатие на объявление в интернете, посещение заряженного сайта может привести к необратимым последствиям работы организации;

Нелицензированное программное обеспечение. Необходимо, чтобы атаки на информационную безопасность организации сводились к минимуму.

Таким образом, в статье проанализированы основные виды угроз и возможность долговременно и незаметно для операторов систем и сетей устранять угрозы безопасности информации. Отмечено, что нарушители с высокими возможностями, имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием не декларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей.

Также были рассмотрены теоретические вопросы, касающиеся общих принципов организации распределенных информационных систем. Была сделана попытка описать и провести анализ современных подходов к организации

распределенных информационных систем, а также рассмотрены вопросы, связанные с программным обеспечением для построения распределенных систем, включая распределенные системы управления базами данных.

Материал, приведенный в статье, даёт понять, что процесс внедрения распределенной информационной системы в организации – это не только приобретение лицензии, но и технологический процесс, состоящий из определенного набора видов деятельности, каждый из которых важен по-своему.

Пренебрежение одним из этих аспектов, таких как выбор клиент-серверных технологий, распределенных систем управления базами данных, а также технологий распределенного программирования и каналов передачи информации, неминуемо приведет к проблемам дальнейшего использования подобных систем.

Литература

1. Федеральный закон от 27.07.2006. № 149-ФЗ (ред. от 12.12.2023.) «Об информации, информационных технологиях и о защите информации» // «Собрание законодательства РФ», 31.07.2006. № 31 (1 ч.), ст. 3448.

2. Баланов А.Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие. М.: Инфра-Инженерия. 2024. 156 с.

3. Зенков А.В. Информационная безопасность и защита информации. М.: Юрайт. 2023. 108 с.

4. Прохорова О.В. Информационная безопасность и защита информации. М.: Лань. 2024. 124 с.

5. Царегородцев А.В., Дербин Е. А. Информационное противоборство. Концептуальные основы обеспечения информационной безопасности. М.: Инфра-М. 2024. 267 с.