АНАЛИЗ ПРОЦЕССА ЗАЩИТЫ ИКС ОТ КОМПЛЕКСНЫХ АТАК

Кенжабаев Бегзод Алиевич
студент
Нукусский филиала Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми

Аннотация: В современном цифровом мире обеспечение комплексной безопасности корпоративной информации становится необходимостью для бизнеса любого масштаба. С ростом числа киберугроз и утончением способов атак на информационные системы предприятий, защита конфиденциальных данных, финансовых ресурсов и репутации компании становится приоритетом. Комплексная безопасность информации охватывает широкий спектр мероприятий, начиная от защиты сетевых инфраструктур и эффективного управления доступом до контроля за передачей данных и обеспечения безопасности приложений.

Ключевые слова: Системы комплексной безопасности, киберугрозы, информационные системы предприятий, защита конфиденциальных данных.

В настоящее время информационная экономика бурно сопровождается активным развитием коммуникационных и информационных технологий, которые также активно влияют на изменение организационных устройств систем управления компанией. С появлением глобальных сетей Интернет меняются традиционные экономические модели ведения бизнеса: основными преобразованиями компаний становятся выравнивание деятельности, децентрализация, а также повышение гибкости. Предприятие становится более капиталоемким, наукоемкая продукция используется чаще, в большей степени определяется состояние как экономики, так и общества в целом. В сопровождении информационной экономики можно наблюдать информационный кризис, отрицательным последствием которого считается информационный «голод», который, в свою очередь, негативно отражается на развитии информационных ресурсов компании.

Сегодня индустрия информационных технологий, услуг и т.п. занимает доминирующее положение – это является главной причиной преобразования экономики в информационную, так как информация – это основной производственный ресурс, находящийся наравне с энергией, материалами, финансами. Основной фактор трансформации экономики в информационную

– это развитие коммуникационных и информационных технологий во всех ее сферах.

Создание, внедрение и становление информационных ресурсов в компании осуществляется по таким направлениям как:

• Определение проблем и формулировка информации, которая необходима для решения данных проблем;

• Изучение источников необходимой информации;

• Сбор, обработка и анализ информации, которая необходима для решения найденных проблем;

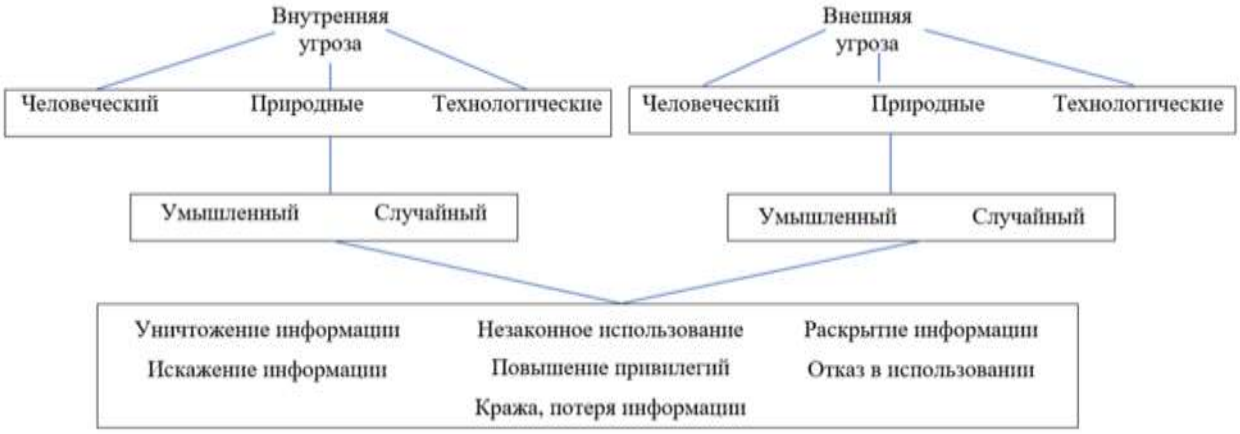
• Разработка и оценка задач для сотрудника, принимающего решение.

Также ключевым моментом для внедрения современных способов ведения бизнеса является безопасность компании, так как она неотделима от устранения проблем информационной безопасности [2].

Информационные технологии – это методы и процессы сбора, обработки, хранения, предоставления и распространения информации, а также способы осуществления таких методов и процессов. Специалисты, занимающиеся в данной сфере, называются IT- или ИТ-специалистами.

На самом деле информационные технологии охватывают абсолютно все области поиска, сбора, хранения, передачи и восприятия любой информации, при этом, не ограничиваясь лишь компьютерными технологиями. Сейчас информационные технологии часто ассоциируются с компьютерными, так как появление компьютеров способствовало выходу ИК-технологий на новый уровень[3].

Мы классифицируем угрозы безопасности, которые могут повлиять на систему, в соответствии с пятью основными критериями, ведущими к нескольким элементарным классам угроз, как показано на рисунке 1.2. В нашей модели классификации угроз мы учитываем следующие критерии: источник, агент, мотивация, намерение и последствия.



Угрозы классифицируется, во-первых, по их источнику. Фактически угроза возникает либо внутри организации, либо из внешней точки происхождения. Действительно, экологические угрозы бывают либо внутренними,

обусловленными природными процессами, либо внешними, обусловленными природными процессами, возникающими за пределами системных границ. Кроме того, экологические угрозы естественны и поэтому возникают без злонамеренных целей, а допущенные ошибки обусловлены непреднамеренными действиями.

Рисунок. 1.2. Модель классификации многомерных угроз

Действия человека различают по цели пользователя при его использовании: вредоносные и незлонамеренные угрозы. Кроме того, вредоносные и незлонамеренные угрозы можно разделить в зависимости от намерений злоумышленника: случайные и преднамеренные угрозы. Технологические угрозы вызваны физическими и химическими процессами, происходящими в материале. Эти угрозы внедряются без злонамеренных целей, а допущенные ошибки обусловлены непреднамеренными действиями.

Модель включает в качестве последнего критерия воздействие угроз. Мы разделяем воздействие угроз на семь типов: уничтожение информации, повреждение информации, кража или потеря информации, раскрытие информации, отказ в использовании, повышение привилегий и незаконное использование. Угроза безопасности может привести к одному или нескольким разрушительным воздействиям на системы.

Источник угрозы безопасности. Угроза может быть вызвана внутренними, внешними или внешними и внутренними объектами. Ниже концентрируемся только на бинарной классификации происхождения угроз: внутренние или внешние, чтобы локализовать происхождение (или источник) угрозы.

Внутренние угрозы возникают, когда кто-то имеет авторизованный доступ к сети либо с помощью учетной записи на сервере, либо с физическим доступом к сети. Угроза может быть внутренней для организации в результате действий сотрудников или сбоя в организационном процессе. Внешние угрозы могут исходить от отдельных лиц или организаций, работающих за пределами компании. У них нет авторизованного доступа к компьютерным системам или сети. Наиболее очевидными внешними угрозами компьютерным системам и резидентным данным являются стихийные бедствия: ураганы, пожары, наводнения и землетрясения. Внешние атаки происходят через подключенные сети (проводные и беспроводные), физическое вторжение или партнерскую сеть.

Агент угроз — это субъект, создающий угрозу системе. Мы выделили три класса для нашей конкретной классификации: люди, стихийные бедствия и технологические угрозы. Предлагаемая классификация охватывает весь набор потенциальных агентов, поскольку включает в себя человека, химическую и физическую реакцию на рукотворные объекты (технологические), а также, естественно, все те агенты, на которые человек не оказывает никакого влияния. Этот класс включает угрозы, вызванные действиями человека, например инсайдеров или хакеров, которые причиняют вред или подвергают риску системы. Экологические угрозы – это угрозы, вызванные нечеловеческими факторами. Во-первых, это происходит из-за угроз стихийных бедствий, таких как землетрясения, наводнения, пожары, молнии, ветер или вода, а также из-за животных и диких животных, которые наносят серьезный ущерб информационным системам, таких как наводнения, молнии, приливные волны (например, цунами) и пожары. Действительно, в этот класс входят и другие угрозы, такие как беспорядки, войны и террористические атаки [11]. Технологические угрозы вызваны физическими и химическими процессами, происходящими в материалах. Физические процессы включают использование физических средств для проникновения в зоны с ограниченным доступом, такие как здание, общее помещение или любую другую специально отведенную зону, например, кража или повреждение оборудования и программного обеспечения. Однако химические процессы включают в себя аппаратные и программные технологии. Оно также включает в себя оборудование косвенной поддержки системы, такое как источники питания [11].

В области обеспечения безопасности информационных систем комплексный подход играет решающую роль, создавая защищенную среду

для обработки данных и обеспечивая определенный уровень безопасности. Этот подход, хотя и обладает ключевыми преимуществами, такими как надежность и комплексность мер, также имеет свои недостатки, включая ограничения для пользователей и сложность управления защитными механизмами. Он применяется как в крупных корпоративных системах, так и в небольших организациях, где безопасность данных играет важную роль.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Seitnazarov K.K. Integration of gis technology for fuzzy deterministic simulation of conditions of operation and maintenance Kegeyli groundwater is abstracted// «IJRET» Volum 4 Issue 2. – Indiya, 2015. – P.727-735. eISSN: 2319-1163/pISSN: 2321-7308.
2. Усманов Р.Н., Сеитназаров К.К. Об организации параллельных вычислений в процессе решения геофильтрационных задач // Вестник ТУИТ. – Ташкент, 2014. - № 1. – С. 101-106. ISSN 2010-9857
3. Usmanov R.N., Seitnazarov K.K. The problem of information model development for the relationship between hydrogeological object and its fuzzy-deterministic model// The Advanced Science Journal. USA, 2014 –№7. – С.67-73. ISSN 2219-746X.
4. Усманов Р.Н., Сеитназаров К.К. Программный комплекс нечетко-детерминированного моделирования гидрогеологических объектов // Автоматика и программная инженерия. – Новосибирск, 2014. – № 1. – С. 29-34. ISSN 2312-4997.
5. Усманов Р.Н., Сеитназаров К.К. Нечетко-детерминированные математические модели процессов восстановления запасов и качества подземных вод // Наука и мир. – Волгоград, №5(21), 2015 – С. 102-104. ISSN 2308-4804.
6. К.К.Сеитназаров, Б.К.Туремуратова. Разница Между Глубоким И Машинным Обучением // Periodica Journal of Modern Philosophy, Social …, 2022
7. К.К.Сеитназаров, Б.К.Туремуратова. ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМЕ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ// Новости образования: исследование в XXI веке, 2022.
8. К.К. Сеитназаров, Д.Х. Турдышов, Б.К. Туремуратова. ОБЗОР МЕТОДОВ ПОЛУЧЕНИЯ КОСМИЧЕСКИХ ИЗОБРАЖЕНИЙ С ВЫСОКИМ РАЗРЕШЕНИЕМ// НАУКА и ОБЩЕСТВО

9. K. Seitnazarov, D. Turdishov, A. Dosimbetov. Knowledge base of algorithmic software complex for providing agricultural fields with water resources// AIP Conference Proceedings, 2024.

10. K.K. SEITNAZAROV, B.M. MAMBETKARIMOV. DEVELOPMENT AND APPLICATION OF A DIGITAL EDUCATIONAL RESOURCE FOR TEACHING PROGRAMMING IN HIGHER EDUCATION INSTITUTIONS// Mental Enlightenment Scientific-Methodological …, 2024.

11. K.K. Seitnazarov, A.K. Bazarbaeva.METHODOLOGY FOR ASSESSING THE ECTS CREDIT SYSTEM IN HIGHER EDUCATIONAL INSTITUTIONS IN WESTERN EUROPE//Modern Science and Research 3 (2), 728-731.

12. К.К. Сеитназаров, Н.С. Мухиятдинов, М.М. Урынбаева. Искусственный интеллект и его применение в принятии решений: методы, алгоритмы и перспективы// Journal of Universal Science Research, 2023.

13. Seitnazarov K.K. Dosımbetov A.M., Aytanov A.K., Omaraov X./ Software Principles for Mapping the Relative State of Groundwater/ European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 7, Issue 11, 2020. – P 319-323.

14. Seitnazarov K.K. Dosımbetov A.M., Aytanov A.K/ Strategy for Organization of Computational Experiments of the Functioning of Underground Water Inlets Using a Fuzzy Multiple Approach/ 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2020, pp. 1-4.

15. Seitnazarov K.K. Aytanov A.K.., Kojametov E., Asenbaev N./ 2021 International Conference on Information Science and Communications Technologies (ICISCT)./ Hydrogeological-Mathematical Model of Formation and Management of Resources and Quality of Fresh Underground Water of the Karakalpak Artesian Basin.

16. Kalimbetov K. I., Turemuratova B. K., Bekbergenova A. B. The structure of fuzzy multiple model of assessing students' knowledge, skills and qualification in higher education //INTERNATIONAL JOURNAL OF SOCIAL SCIENCE & INTERDISCIPLINARY RESEARCH ISSN: 2277-3630 Impact factor: 7.429. – 2022. – Т. 11. – С. 4-8.

17. Сеитназаров К. К. и др. ОБЗОР МЕТОДОВ ПОЛУЧЕНИЯ КОСМИЧЕСКИХ ИЗОБРАЖЕНИЙ С ВЫСОКИМ РАЗРЕШЕНИЕМ //НАУКА и ОБЩЕСТВО. – С. 28.