Шумилина В.Е., к.э.н., доцент кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;

Лагутин Д.А., студент 3-го курса кафедры «Экономическая безопасность, учет и право» ДГТУ, Ростов-на-Дону, Россия;

ОБ ОСОБЕННОСТЯХ И ПРИНЦИПАХ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Аннотация. В данной статье рассматривается важность создания и реализации системы управления информационной безопасностью. Приводится статистика того, какие конкретно зоны подвержены массовым атакам в 2021 году, а также предложены способы, чтобы обеспечить дополнительную безопасность информации и минимизировать шансы ее утери.

Ключевые слова: информационная безопасность, система управления информационной безопасностью, обеспечение защиты информации, системы защиты информации, сегментация.

Shumilina V.E., Candidate of Economics, Associate Professor Department of economic security, accounting and law of the DSTU Rostov-on-Don, Russia;

Lagutin D.A., 3rd year student of the department "Economic security, accounting and law", Don State Technical University, Rostov-on-Don, Russia;

ON THE FEATURES AND PRINCIPLES OF AN INFORMATION SECURITY MANAGEMENT SYSTEM

Annotation. This article discusses the importance of establishing and implementing an information security management system. It provides statistics on which specific areas are prone to mass attacks in 2021, and suggests ways to provide additional information security and minimize the chances of information loss.

Keywords: information security, information security management system, information assurance, information protection systems, segmentation.

Достижение полной и бесперебойной работы системы управления информационной безопасностью сегодня – ключевая задача каждого предприятия. Данный механизм минимизирует возникающие риски. В настоящее время бизнес имеет потребность в защите собственной информации. Все это приводит к тому, что необходимо создание обеспечения информационной безопасности предприятия. Она нацелена, в первую очередь, на обеспечение информационной безопасности.

Современные подходы к обеспечению информационной безопасности предполагают наличие, с определенного уровня зрелости организации, процессов управления информационной безопасностью, и как следствие - системы управления информационной безопасностью. Данный механизм представлен в виде части системы управления, основанной на использовании методов оценки бизнес-рисков для следующих операций:

- разработки;

- внедрения;

- мониторинга;

- анализа;

- функционирования;

- поддержания стабильной работы информационной безопасности всего предприятия.

Цель создания данной системы кроется в выборе соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон. Процессы управления должны выполнять следующие функции:

- оценка эффективности системы;

- прогнозирование и анализ работы системы;

- превентивное обнаружение неисправностей в системе обеспечения информационной безопасности;

- реагирование на изменение бизнес-процессов.

Важным этапом в данном вопросе является работа над созданием концепции безопасности объекта. Под концепцией безопасности объекта понимается обобщение системы взглядов на задачу обеспечения безопасности защищаемого объекта на различных этапах и уровнях его функционирования, определения основных принципов построения системы, разработки направлений и этапов реализации мер безопасности.

Принципы построения системы безопасности

Принцип законности. Реализация этого принципа осуществляется за счет тщательного соблюдения и выполнения при разработке и построении систем безопасности положений и требований действующего законодательства и нормативных документов.

Принцип своевременности. Реализуется принятием упреждающих мер, направленных на обеспечение безопасности объекта защиты.

Принцип совмещения комплексности, эффективности и экономической целесообразности. Реализуется за счет построения системы безопасности, обеспечивающей надежную защиту объекта от возможных угроз с минимально возможными затратами.

Принцип модульности и интегративности. Реализуется за счет построения системы на базе гибких аппаратно-программных модулей. Модульность и интегративности системы безопасности позволяет наращивать, изменять конфигурацию системы и вносить другие изменения без замены основного оборудования.

Принцип иерархичности. Реализуется за счет построения многоуровневой структуры. Модульность, интегративность и иерархичность позволяют разрабатывать системы безопасности для самого высокого организационно - структурного уровня.

Принцип совместимости технологических, программных, информационных, конструктивных, энергетических и эксплуатационных элементов в применяемых технических средствах. Технологическая совместимость обеспечивает технологическое единство и взаимозаменяемость компонентов. Это требование достигается унификацией технологии производства составных элементов системы. Информационная совместимость подсистем систем безопасности обеспечивает их оптимальное взаимодействие при выполнении заданных функций.

Достижение поставленной цели осуществляется путем реализации следующих основных задач системы безопасности объекта защиты:

- создание системы, способной своевременно реагировать на возникающие угрозы безопасности;

- организация защиты для собственных ресурсов кампании для предотвращения их утечки в случае несанкционированного проникновения в систему;

- защита жизни и здоровья лиц, находящихся на объекте, защита материальных и информационных ценностей, путем своевременного выявления и устранения угроз;

- создание условий для максимально возможного восстановления ущерба, полученного в результате нарушения безопасности.

Необходимо также уделить отдельное внимание системе защиты информации, поскольку она является важнейшим ресурсом предприятия, особенно, если это коммерческая тайна организации. Сегментирование информационной системы проводится на основании сведений об общности категории обрабатываемой информации, процессов обработки, физического расположения локальной вычислительной сети, юридического подчинения (крупные организации нередко включают в себя несколько юридических лиц).

Использование принципа сегментации позволяет получить следующие преимущества:

- повышение надежности сети за счет изолирования инцидентов в сегменте;

- ограничение доступа за пределы сегмента;

- упрощает управление защитой.

Сегментирование может осуществляться посредством использования разнообразных средств:

Управление событиями ИБ включает в себя процессы:

- регистрации;

- сбор; хранения;

- защиты;

- мониторинга;

- анализа.

Результаты процесса управления событиями лежат в основе процессов обнаружения инцидентов и совершенствования системы защиты информации.

Согласно статистическим данным CyberPolygon, в 2021 году доминирующими были классические атаки – фишинговые сайты на тему коронавируса, оформление якобы подлинных документов о вакцинации, мошеннические операции с услугами, реклама проектов, приносящих мгновенных доход. Такие злонамеренные действия составили более 85 % атак. Примерно 10 % атак, зафиксированных в 2021 году, пришлись на программы-вымогатели, которые были нацелены на корпорации. Наиболее известный пример – атака на ColonialPipeline, из-за чего оказалась парализованной гигантская сеть заправок в США. И меньше всего атак было, не более 5 %, таргетированного характера, чрезвычайно хорошо организованные, направленные на государственные структуры разных стран. Они до сих пор полностью не расследованы.

В компании Ростелеком-Солар предоставили свою статистику. Согласно ей фишинг в 2021 году был самым известным методом, используемым преступниками низкой квалификации. Таких атак было зафиксировано не менее 60 %. Хакеры более высокого уровня подготовки эксплуатировали веб-уязвимости государственных органов власти. Таких атак было в 2021 году 50 %.

Пандемия привела не только к росту инфляции и сбою логистики в мире, но и вызвала сокращение затрат на обеспечение информационной безопасности. Особенно это было заметно в государственных органах власти на местных уровнях и у компаний с небольшими бюджетами.

К таким проблемам относятся следующие:

- Региональные коммерческие и государственные площадки не имеют должного уровня защиты.

- IT-администраторы и подрядчики не обладают соответствующей квалификацией, не совершенствуют протоколы безопасности.

- Средства защиты устаревшие, не обновляются, к ним есть широкий доступ.

- Критичные обновления почти не устанавливаются в органах власти, особенно в регионах.

- Персонал обладает слабой подготовкой, не выполняет элементарных требований по безопасности.

- Ощущается значительная нехватка специалистов по информационной безопасности, поскольку они уже заняты в других проектах.

- Имеется малое количество персонала, полностью осведомленного во всех тонкостях реализации информационной безопасности. Нет согласованности между ведомствами в противодействии угрозам преступников.

- Из-за нехватки средств не обновляется ПО для защиты. Без их решения крайне трудно противостоять атакам на систему безопасности информации, хотя уже создаются новые и эффективные методы защиты.

Базовые основы для защиты собственной информации:

- Сложные пароли. Не рекомендуется хранить информацию о паролях на ПК, используемого для работы в сети. Обязательно нужно использовать двухэтапную аутентификацию, это обеспечит повышенную защиту аккаунта;

- Проверка политики конфиденциальности.Перед тем, как устанавливать расширения на браузеры, приложения, регистрироваться в них, пользователь обязан изучать политику конфиденциальности. Нужно убедиться в том, что приложения или расширения не имеют права использовать личные данные.

- Настройки браузеров.Пользователь не должен давать браузеру разрешение автоматически запоминать пароли к сайтам. Рекомендуется отключать опцию в настройках. Должна быть отключена синхронизация браузеров на ПК и в смартфонах.

- Очистка cookies.Эксперты рекомендуют регулярно очищать временные файлы, которые содержат сведения о сайтах, посещаемых пользователем. Периодичность очистки должна быть несколько раз в неделю. Так минимизируется риск взлома и доступа к личным данным.

- Общественные Wi-Fi сети.Не рекомендуется использовать открытые общественные сети, поскольку через них можно быстро взломать ПК или гаджет.

- Регулярное обновление антивирусного ПО.Пользователь обязан регулярно обновлять свое антивирусное ПО. Лучше всего устанавливать платные версии антивирусных программ, так как они обладают большим количеством модулей для защиты информации.

Таким образом, можно сделать вывод, что обеспечение информационной безопасности является приоритетной задачей каждого предприятия. В наше время, когда информация является общедоступным феноменом, ее защита является ключевой задачей каждого. Наглядно это демонстрирует предоставленная статистика. Необходимо учитывать все нюансы при построении системы управления информационной безопасностью, а также за ее дальнейшим применением.

Список источников

1. Баскаков А. В., Остапенко А. Г., Щербаков В. Б. Политика информационной безопасности как основной документ организации // Информация и безопасность. – 2018. - №2. – С. 43-47.
2. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2017. - 368 с.
3. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции. Журнал «Вопросы кибербезопасности» №1 (2) – 2019
4. Зефиров С. Л., Голованов В. Б. Система менеджмента информационной безопасности организации // Труды международного симпозиума «Надежность и качество». – 2016. – С. 364-366.
5. Мельников В.П. Информационная безопасность и защита информации: учебное пособие для вузов. - М.: Академия, 2018. - 336 с.
6. Шумилина, В. Е. Управление информационными рисками в организации / В. Е. Шумилина, О. В. Асташова, А. А. Аистова // Наука и мир. – 2021. – № 1. – С. 36-40. – DOI 10.26526/2307-9401-2021-1-36-40. – EDN ZLBFQA.
7. Шумилина, В. Е. Экономическая безопасность предприятий малого и среднего бизнеса / В. Е. Шумилина, А. А. Борзых // Управление безопасностью бизнеса в современных условиях. – Москва : AUSPUBLISHERS, 2021. – С. 74-83. – EDN WBPPMN.
8. Шумилина, В. Е. Основные проблемы защиты конфиденциальной информации и пути их решения / В. Е. Шумилина, Ю. И. Коптева, С. А. Тевосян // : Современные проблемы экономической безопасности,

учета и права в Российской Федерации. Том 3, 11 января 2018 года – 31 2019 года, 2019. – С. 9. – DOI 10.26526/conferencearticle_5c5060d2f3afe7.25271992. – EDN YWPACT.

References

1. Baskakov A. V., Ostapenko A. G., Shcherbakov V. B. Information security policy as the main document of an organization // Information and security. - 2018. - No. 2. – P. 43-47.
2. Security and access control in information systems: Textbook / A.V. Vasilkov, I.A. Vasilkov. - M.: Forum: NIC INFRA-M, 2017. - 368 p.
3. Dorofeev A.V., Markov A.S. Information security management: basic concepts. Journal "Cybersecurity Issues" No. 1 (2) - 2019
4. Zefirov S. L., Golovanov V. B. Information security management system of an organization // Proceedings of the international symposium "Reliability and quality". - 2016. - S. 364-366.
5. Melnikov V.P. Information security and protection of information: a textbook for universities. - M.: Academy, 2018. - 336 p.
6. Shumilina, V. E. Management of information risks in an organization / V. E. Shumilina, O. V. Astashova, A. A. Aistova // Science and World. - 2021. - No. 1. - P. 36-40. – DOI 10.26526/2307-9401-2021-1-36-40. – EDN ZLBFQA.
7. Shumilina, V. E. Economic security of small and medium-sized businesses / V. E. Shumilina, A. A. Borzykh // Management of business security in modern conditions. - Moscow: AUSPUBLISHERS, 2021. - S. 74-83. – EDN WBPPMN.
8. Shumilina, V. E. The main problems of protecting confidential information and ways to solve them / V. E. Shumilina, Yu. I. Kopteva, S. A. Tevosyan //: Modern problems of economic security, accounting and law in the Russian Federation. Volume 3, January 11, 2018 - January 31, 2019, 2019. - P. 9. -

DOI 10.26526/conferencearticle_5c5060d2f3afe7.25271992. – EDN YWPACT.