В курсе экономики предприятия имущество рассматривается как хозяйственный, экономический ресурс, использование которого обеспечивает успешную деятельность предприятия.

Таким образом, имущество организации является важным объектом бухгалтерского учета, который требует правильной оценки, классификации и учета движения. Корректный учет имущества позволяет организации оптимизировать свои расходы и управлять своими ресурсами эффективно.

СПИСОК ЛИТЕРАТУРЫ

1 Имущество организации как объекты бухгалтерского учета [Электронный ресурс]. – Режим доступа : https://studfile.net/preview/9005675/page:9/. – Дата доступа : 28.04.2023.

2 Основы бухгалтерского учета имущества организации [Электронный ресурс]. – Режим доступа : https://studwood.net/1545634/buhgalterskiy_uchet_i_audit/osnovy_buhgalterskogo_ucheta_imuschestva_organitsii. – Дата доступа : 28.04.2023.

3 Имущество организации как объекты бухгалтерского учета и их классификация [Электронный ресурс]. – Режим доступа : https://infopedia.su/11x679f.html. – Дата доступа : 29.04.2023.

4 Бухгалтерский учет : учеб. [Электронный ресурс] / под ред. А. А. Коровкина. – М. : ИНФРА-М, 2019. – Режим доступа : https://www.biznesbooks.com/components/com_jshopping/files/demo_products/yu-a-babaev-i-p-komissarova-v-a-borodin-bukhgalterskij-uchet.pdf. – Дата доступа : 29.04.2023.

5 Имущество компании: понятие, состав и налогообложение [Электронный ресурс]. – Режим доступа : https://www.gd.ru/articles/10211-imushchestvo-kompanii. – Дата доступа : 29.04.2023.

Получено 31.05.2023

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 28. Гомель, 2023

УДК 004.056

Т. В. ЗАЙЦЕВА (ЗмТ-56)
Научный руководитель – магистр, ст. преп. *С. В. КИСЕЛЁВА*

ОЦЕНКА УРОВНЯ УГРОЗ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Изучены самые распространенные виды угроз за предыдущий год. Произведен анализ статистики отчета 2022 г., предоставленного для общего доступа лабораторией Касперского. Произведена оценка уровня угроз в сфере информационной безопасности организаций к настоящему времени.

Создание современных компьютерных систем и появление глобальных компьютерных сетей радикально изменило характер и диапазон проблем защиты информации. Двадцать лет назад задача обеспечения безопасности информации решалась при помощи средств криптографической защиты, установления межсетевых экранов, разграничения доступа. Сейчас этих технологий недостаточно, любая информация, имеющая финансовую, конкурентную, военную или политическую ценность, подвергается угрозе. Дополнительным риском становится возможность перехвата управления критическими объектами информационной инфраструктуры.

Основными задачами обеспечения информационной безопасности считаются доступность, целостность, включающая аутентичность, а также конфиденциальность. Актуальность угроз целостности и конфиденциальности информации требует внимательного отношения к задаче ее защиты.

Множество систем безопасности в настоящее время являются системами поиска совпадений (сигнатур) и моделей поведения уже известных угроз. Они бессильны против новых атак, на которые еще нет сигнатур и патчей от производителя (автоматизированное отдельно поставляемое программное средство, используемое для устранения проблем в программном обеспечении или изменения его функциональности). Причем новые атаки, как правило, не имеют цели нанести заметного ущерба, а спроектированы для незаметного, скрытного выполнения вредных действий [2].

Анализ инцидентов последних лет позволяет объективно оценивать тенденции киберугроз и методов, которые используют злоумышленники. Проанализируем инциденты в сфере защиты информации за последний год, предоставленные лабораторией Касперского в ежегодных бюллетенях.

На сегодня наиболее опасными и распространенными являются целевые атаки. Целенаправленная атака – это длительный процесс, который нарушает безопасность и позволяет киберпреступнику несанкционированно взаимодействовать с IT-инфраструктурой, избегая обнаружения традиционными средствами защиты. Атака такого рода, направленная на конкретную организацию, может длиться неделями, месяцами или годами и оставаться незамеченной. Все это время киберприступники могут собирать конфиденциальную информацию или вмешиваться в бизнес-процессы организации.

Дело в том, что целевая атака совсем не похожа на типичные компьютерные угрозы или сетевые атаки, так как представляет собой набор целенаправленных действий, контролируемых злоумышленниками вручную на всех стадиях проникновения, что сильно выделяет ее в мире киберугроз.

Участившиеся целевые атаки обостряют проблему обеспечения корпоративной кибербезопасности: потенциальные риски растут, что влечет за собой необходимость пересмотра существующей стратегии защиты организаций.

Ежегодный аналитический отчет Managed Detection and Response освещает результаты анализа инцидентов, выявленных командой Центра мониторинга кибербезопасности (SOC) «Лаборатории Касперского» [1].

Количество критичных инцидентов по отраслям деятельности согласно аналитическому отчету MDR представлено на рисунке 1.

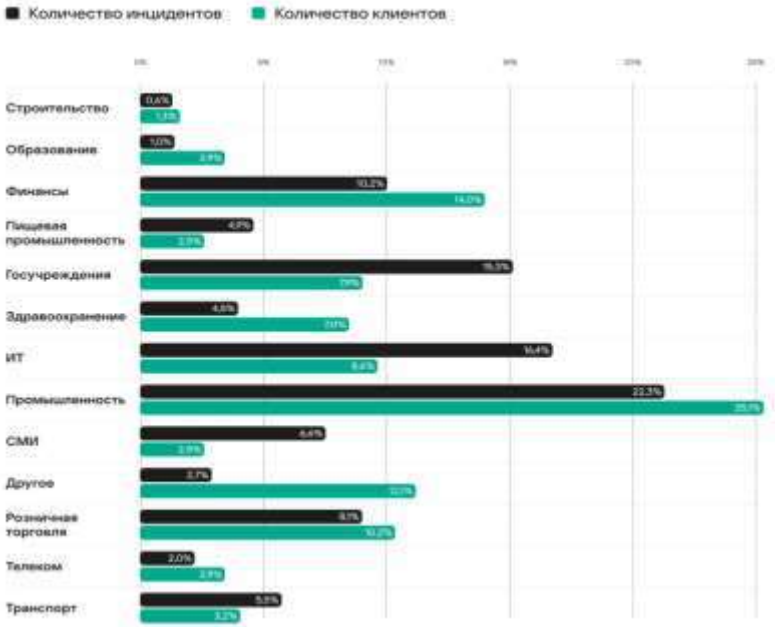

Рисунок 1 – Количество критичных инцидентов по отраслям деятельности

По данным статистики можно сделать следующие выводы:

1 Все типы критичных инцидентов, наблюдаемые за период, фиксировались в государственных учреждениях, ИТ-компаниях, на промышленных предприятиях и в сфере здравоохранения.

2 На всех предприятиях, где фиксировались инциденты с непосредственным участием человека (целевые атаки), также наблюдались и инциденты, связанные с обнаружением следов прошлых целевых атак (за исключением образовательных учреждений, где в 2022 г. фиксировались активные атаки, однако следов прошлых взломов обнаружено не было). Это подтверждает тот факт, что атакующие возвращаются.

3 Статистика активных целевых атак повторяет статистику киберучений, единственное исключение – строительство. Это может свидетельствовать о том, что в большинстве своем компании корректно оценивают риски.

4 Практически во всех индустриях наблюдались инциденты, связанные с В/О (вредоносное ПО) без видимых следов участия человека, исключение – образование и СМИ.

5 Статистика целевых атак во многом схожа с распределением инцидентов, связанных с В/О, исключение составляют образование и СМИ. Это подтверждает наблюдаемую в последнее время тенденцию, что атаки В/О с большим ущербом начинаются как целевые с участием человека: первоначальное проникновение и запуск выполняются вручную, а дальнейшее распространение В/О происходит без участия человека. Ввиду неполного покрытия мониторинга обнаружение происходит на этапах, когда на уровне телеметрии MDR не удается связать вредоносную активность с ранее обнаруженными действиями человека, поэтому регистрируются два несвязанных инцидента: целевая атака и В/О.

Согласно статистике всех выявленных в 2022 г. критичных инцидентов 30 % было связано с целевыми атаками при непосредственном участии человека. Большое количество инцидентов этого типа также может быть связано и с разного рода киберучениями (моделирование реакции на инцидент), так как в обоих случаях наблюдается активная работа атакующего, и по умолчанию они классифицируются как «целевые атаки» и тип инцидента изменяется на «киберучения» только при получении явного подтверждения от заказчика. Атаки вредоносного ПО с серьезными последствиями составили почти 26 %. Киберучения (тестирование на проникновение, учения с участием Red Team и т. п.) превысили 19 %. Около 9 % – доля инцидентов, связанных с публично доступными критичными уязвимостями, и инцидентов, основанных на обнаружении следов ранее активных атак с участием человека (целевые атаки или киберучения). Около 4 % инцидентов – результат успешного использования социальной инженерии с последующим развитием, приведшим к серьезным последствиям.

Немногим менее 4 % инцидентов было связано с внутренними нарушителями.

Современный мир, информационное пространство порождают множество угроз информационной безопасности, с каждым годом наращивая спектр потенциальных угроз и возможности их реализации. Мировая статистика инцидентов в сфере информационной безопасности показывает, что с повышением уровня опасности киберугроз действующие системы защиты нуждаются в периодической актуальной оценке готовности обеспечивать необходимый уровень информационной безопасности организации.

СПИСОК ЛИТЕРАТУРЫ

1 Managed Detection and Response. Отчет за 2022 год [Электронный ресурс]. – Режим доступа : https://securelist.ru/mdr-report-2022/107350/. – Дата доступа : 18.05.22.

2 **Завгородний, В. И.** Комплексная защита информации в компьютерных системах : учеб. пособие / В. И. Завгородний. – М. : Логос, 2001. – 264 с.

Получено 22.05.2023