Министерство науки и высшего образования
Российской Федерации
Тольяттинский государственный университет

Т.А. Раченко

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Электронное учебно-методическое пособие

ISBN 978-5-8259-1612-5

УДК 378.147(075.8)
ББК 74.480.278я73

Рецензенты:
канд. техн. наук, доцент кафедры «Информационный и электронный сервис» Поволжского государственного университета сервиса *Т.С. Яницкая*;
канд. пед. наук, доцент кафедры «Прикладная математика и информатика» Тольяттинского государственного университета *О.А. Крайнова.*

Раченко, Т.А. Информационная безопасность : электронное учебно-методическое пособие / Т.А. Раченко. – Тольятти : Изд-во ТГУ, 2024. – 1 оптический диск. – ISBN 978-5-8259-1612-5.

Учебно-методическое пособие «Информационная безопасность» разработано в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 09.03.03 «Прикладная информатика».

Составлено в соответствии с государственными требованиями к минимуму содержания и уровня подготовки бакалавра.

Может быть полезно преподавателям и инженерно-техническим работникам.

Текстовое электронное издание.

Рекомендовано к изданию научно-методическим советом Тольяттинского государственного университета.

Минимальные системные требования: IBM PC-совместимый компьютер: Windows XP/Vista/7/8/10; PIII 500 МГц или эквивалент; 128 Мб ОЗУ; SVGA; CD-ROM; Adobe Acrobat Reader.

Учебное издание

Раченко Татьяна Александровна

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Редактор *Т.М. Воропанова*
Технический редактор *Н.П. Крюкова*
Компьютерная верстка: *Л.В. Сызганцева*
Художественное оформление,
компьютерное проектирование: *И.И. Шишкина*

Электронное учебно-методическое пособие предназначено
для использования в образовательной деятельности
исключительно в некоммерческих целях.

В оформлении пособия использованы изображения
от Freepik и bedneyimages на сайте ru.freepik.com

Дата подписания к использованию 20.02.2024.
Объем издания 3,4 Мб.
Комплектация издания: компакт-диск,
первичная упаковка.
Тираж 50 экз. Заказ № 1-10-23.

Издательство Тольяттинского государственного университета
445020, г. Тольятти, ул. Белорусская, 14,
тел. 8 (8482) 44-91-47, www.tltsu.ru

Содержание

ВВЕДЕНИЕ

Учебно-методическое пособие «Информационная безопасность» предназначено для студентов, обучающихся по направлению укрупненной группы направлений подготовки 09.03.03 «Прикладная информатика». Пособие может также использоваться студентами других направлений и специальностей при изучении вопросов, связанных с кибербезопасностью.

В пособии рассмотрена система управления кибербезопасностью в современной цифровой организации. Дан краткий анализ моделей и политики безопасности, связанных с защитой информации в информационных (автоматизированных) системах. В учебно-методическом пособии определены как теоретические, так и практические основы классификации и оценки угрозы информационной безопасности; классификации и оценки угроз безопасности информации для объекта информатизации; формирования моделей угроз безопасности компьютерных систем. Особое внимание уделено действующей законодательной базе в области обеспечения защиты информации; анализу событий, связанных с защитой информации в информационных (автоматизированных) системах; использованию криптографических методов и средств защиты информации в автоматизированных системах. Практическая реализация систем безопасности рассмотрена на практике Сбербанка.

Понимание научного подхода в построении защищенных систем необходимо для изучения программно-аппаратных, организационно-правовых, технических методов обеспечения информационной безопасности. Разработка и внедрение в организацию мер кибербезопасности будет способствовать умелым действиям в решении практических вопросов защиты информации в профессиональной деятельности.

Целью освоения дисциплины является формирование знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи изучения дисциплины:

1. Понимать сущность информационной безопасности.
2. Понимать принципы организации защиты информации на предприятиях.

3. Выявлять основные виды угроз информационной безопасности.
4. Применять программно-аппаратные средства для обеспечения информационной безопасности.

После изучения дисциплины студент должен

✓ *знать*:

– основы информационной безопасности и защиты информации;
– принципы криптографических преобразований;
– типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду;
– виды угроз ИС и методы обеспечения информационной безопасности;

✓ *уметь*:

– выявлять угрозы информационной безопасности;
– обосновывать организационно-технические мероприятия по защите информации в ИС;
– реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития программного обеспечения вычислительных систем и разработки средств и систем защиты информации;

✓ *владеть навыками* работы с программными и аппаратными средствами, обеспечивающими защиту информации в компьютерных системах;

✓ *иметь представление* о типовых средствах защиты информации и возможностях их использования в реальных задачах создания и внедрения информационных систем.

Учебно-методическое пособие состоит из двух частей: теоретической части, которая представляет сгруппированный теоретический материал по девяти темам дисциплины, и практических работ, необходимых для изучения программных, аппаратных средств, а также инструментария, необходимого для обеспечения нужного уровня защиты информации в организации.

Тема 1. СИСТЕМА УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ СОВРЕМЕННОЙ ЦИФРОВОЙ ОРГАНИЗАЦИИ

Форма проведения занятия – лекция.

Вопросы для обсуждения

1. Подходы при построении системы управления кибербезопасностью организации.
2. Основные процессы ITSM.

Методические указания по проведению занятия

При освоении темы необходимо:

1. Изучить учебный материал по теме 1.
2. Акцентировать внимание на основополагающих понятиях и определениях.
3. Ответить на контрольные вопросы.

Методическое оборудование к занятию: проектор, ноутбук.

Рекомендуемая литература

1. Кийко, П. В. Цифровые технологии : учеб. пособие / П. В. Кийко ; Омский государственный аграрный университет имени П.А. Столыпина. – Омск : ФГБОУ ВО Омский ГАУ, 2023. – 108 с. – URL: e.lanbook.com/book/349799 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-907687-34-9.
2. Надёжность и защита информации автоматизированных систем : учеб. пособие / М. Н. Краснянский, В. Г. Матвейкин, А. В. Затонский [и др.] ; Тамбовский государственный технический университет. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2022. – 95 с. – URL: e.lanbook.com/book/355145 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8265-2460-2.

Краткие теоретические сведения

В 2018 г. ущерб от деятельности хакеров для мировой экономики и бизнеса оценивался в 1,5 триллиона рублей. Сегодня эта сумма приближается к 10 триллионам.

Каждый год происходят крупные инциденты. Они являются триггерами для того, чтобы сотрудники, ответственные за кибербезопасность, усиливали защиту организаций. Зачастую инциденты связаны с ошибками сотрудников, профессиональных защитников или ИТ-специалистов.

В современном мире невозможно выполнять профессиональные обязанности без выравнивания системы знаний.

Несмотря на то, что вузы готовят достаточно большое количество выпускников в этой области, ситуация в обеспечении рынка кадрами кардинально не меняется. Одна из причин – взрывной рост ИТ-технологий, для которых требуются специалисты, отвечающие современным требованиям.

В чем разница между информационной безопасностью и кибербезопасностью?

Сегодня термин «кибербезопасность» прочно вошел в нашу жизнь. В государстве появились документы, которые его используют. Информационная безопасность устойчива.

Есть соответствующие документы регуляторов, которые определяют требования к ее организации, составу системы управления, необходимости реализации тех или иных мер. Но сегодня современный цифровой мир внес в информационную безопасность и ИТ-технологии два элемента, которые существенно меняют представление о безопасности (рис. 1).

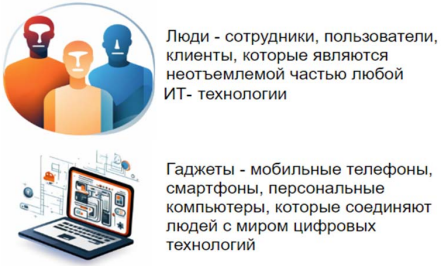


Рис. 1. Элементы ИБ

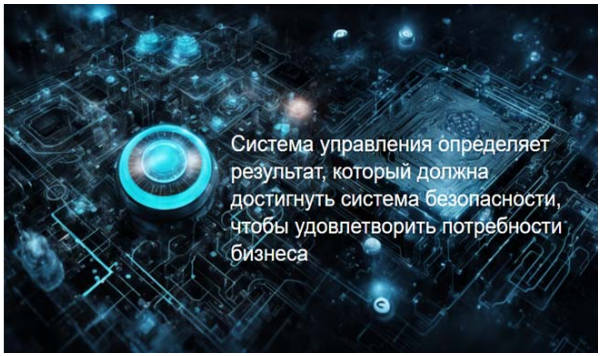
Для любой организации существуют внешние силы, которые могут нарушить стабильность и безопасность ее работы:

• **регуляторы**, которые предъявляют различные требования;

• **клиенты и партнеры**, которые подключаются к инфраструктуре организации и тем самым начинают прямо или косвенно влиять на технические системы организации;

• **дочерние компании**, которые образуют экосистему, являются потенциальной угрозой атаки через цепочки поставок;

• **злоумышленники**, которые используют различные технические каналы и средства, чтобы нарушить деятельность компании.



Факторы, определяющие необходимость подразделений кибербезопасности в организации:

1. Готовность компании развивать собственную экспертизу.
2. Размер организации.
3. Уровень критичности вопросов кибербезопасности.
4. Скорость решения задач защиты информации.
5. Вопросы доверия.

В последнее время на фоне дефицита кадров специалистов кибербезопасности организации вопросы безопасности вынуждены передавать в подрядные организации – «Виртуальный офицер безопасности».

Необходимость разработки и внедрения в организацию мер кибербезопасности:

1. Экстренные необходимые меры, принимаемые с целью минимизации рисков. 99 % всех проблем решается тремя мерами:

- контроль доступа, в том числе установка межсетевых экранов;
- правила доступа и настройка антивирусных средств на всех хостах и рабочих станциях;
- установка обновлений.

2. Если в организации это все приведено к текущему моменту, то реализовывается пересмотр существующих практик и подходов. Системы управления рисками – приоритизации рисков.

У каждой организации есть свои особенности, паритеты бизнеса, бизнес-риски. Начальник отдела безопасности начинает оценку риска исходя из сферы деятельность организации. Например, если это интернет-магазин, который устойчиво работает, но для него критичны надёжность и доступность, потому что именно на этих качествах строится основа бизнеса. В паритете будут мероприятия, направленные на развитие устойчивости от различных атак и сети Интернет.

Контрольные вопросы

1. Какая структура не входит в число регуляторов российских финансовых организаций в области кибербезопасности?
2. Какой слой в структуре системы управления кибербезопасности выделяется в последнее время в качестве отдельного?
3. Какие подходы могут применяться при построении системы управления кибербезопасностью организации?
4. Какой процесс ITSM необходимо внедрять в первую очередь при построении системы кибербезопасности в организации?
5. Какие стадии кибератаки рассматриваются в модели Kill Chain?

Тема 2. ТРЕНДЫ КИБЕРБЕЗОПАСНОСТИ

Форма проведения занятия – лекция.

Вопросы для обсуждения

1. Тенденции DLP, Identity & Access Management, мобильной ИБ, облачные тенденции.
2. Аналитика как функция продуктов по информационной безопасности.

Методические указания по проведению занятия

При освоении темы необходимо:

1. Изучить учебный материал по теме 2.
2. Акцентировать внимание на основополагающих понятиях и определениях.
3. Ответить на контрольные вопросы по теме 2.
4. Выполнить тест по теме 2.

Методическое оборудование к занятию: проектор, ноутбук.

Рекомендуемая литература

1. Журавлёва, Н. А. Экономическая безопасность : учеб. пособие / Н. А. Журавлёва ; Петербургский государственный университет путей сообщения Императора Александра I. – Санкт-Петербург : ФГБОУ ВО ПГУПС, 2022. – 78 с. – URL: e.lanbook.com/book/224522 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-7641-1682-2.
2. Надёжность и защита информации автоматизированных систем : учеб. пособие / М. Н. Краснянский, В. Г. Матвейкин, А. В. Затонский [и др.] ; Тамбовский государственный технический университет. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2022. – 95 с. – URL: e.lanbook.com/book/355145 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8265-2460-2.

Краткие теоретические сведения

Организации думают об информационной безопасности по трем причинам:

1. Страх угрозы, реализации и последствий инцидента или кибератаки.

2. Compliance – угроза невыполнения требований законодательства. Специфична либо для конкретной отрасли, либо для государства в целом.

3. Бизнес – проблема информационной безопасности сужается до уровня конкретной организации. В одной организации ущерб от инцидента может быть существенным, в другой – нет, а в третьей – борьба с ним не предусмотрена, а затраты на последствия от ущерба заложены в себестоимость продукта/услуги.

Каждая компания имеет определенный уровень зрелости обеспечения информационной безопасности (рис. 2).

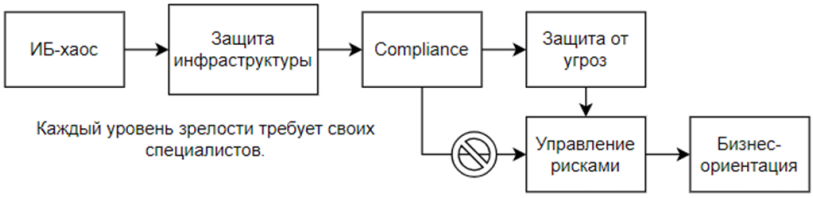


Рис. 2. Уровни зрелости обеспечения информационной безопасности

На финальном уровне компания из каждого направления деятельности извлекает прибыль и находит преимущества для бизнеса. Каждый уровень зрелости требует своих специалистов.

Мировая нехватка специалистов по кибербезопасности составляет 3 миллиона человек. В России – около 60 тысяч при ежегодной подготовке порядка 18 тысяч (по состоянию на июль 2022 г.).

На сегодняшний день безопасность перемещается в сторону сервисной модели.

В сервисной модели обеспечение безопасности осуществляется аутсорсинговой компанией, а на специалиста по безопасности возлагается контроль данных процессов. Есть версия, что через пару лет до 90 % рынка кибербезопасности в России будет реализовано

в виде сервисной модели в связи с массовым уходом иностранных компаний.

Российские компании не могут обеспечить достаточного объема рынка собственными решениями. Сервисная модель позволяет использовать привычные технологии, не афишируя их иностранное происхождение, а в условиях нехватки персонала зачастую является единственным решением задачи.

На кибербезопасность финансовой организации влияют области, показанные на рис. 3.

Рис. 3. Области воздействия на финансовую организацию

Изменения в бизнесе автоматически влекут изменения кибербезопасности. Так, внедрение виртуальных помощников подразумевает решение вопросов защиты самих помощников, интернета вещей и технологий машинного обучения.

Существуют технологии, которые защищают IT-инфраструктуру (файерволы на периметре, VPN для защиты каналов связи, DLP-системы для мониторинга коммуникаций в поисках утечек информации), а есть более крупный пласт задач, технологий и механизмов защиты, интегрированных в бизнес. Они имеют схожую структуру:

– угрозы;
– законодательство;
– IT-технологии;
– бизнес-процессы.

Безопасность сегодня является интегрированной, что больше способствует обеспечению информационной безопасности.

В первую очередь это касается угроз. Необходимо знать, как действуют хакеры.

Защита от угроз

Выделяются четыре основных типа злоумышленников (рис. 4):

1. Инсайдеры.
2. Хактивисты.
3. Киберкриминал.
4. Хакеры на службе государства.

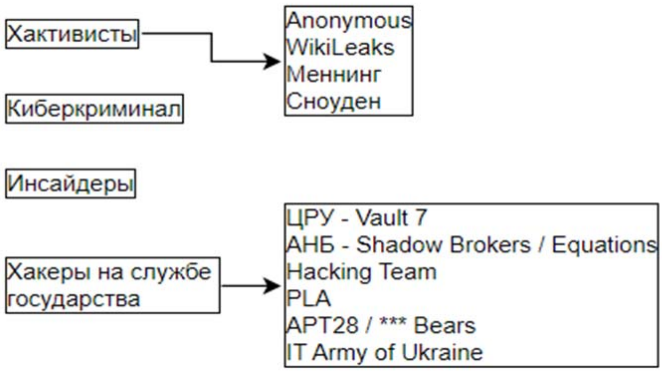


Рис. 4. Типы злоумышленников

Хакерство – это полноценный бизнес, занимающий третье место по объему рынка и имеющий:

- различные механизмы генерации прибылей;
- собственную валюту и инструменты ее обмена и обналичивания;
- различных экономических агентов (поставщики, производители, покупатели);
- широкий продуктовый ряд;
- особые экономические зоны;
- найм персонала;
- собственные торговые площадки;
- глобальные механизмы дистрибуции;
- саморегулирование;
- специальный инструментарий (техподдержка, обучение и повышение квалификации);
- психологов и физиологов.

Рынок киберпреступности будет развиваться. Государство не способно бороться с ним по следующим причинам:

- бюрократизированность;
- необходимость соблюдать требования закона, в отличие от преступников.

Ключевые угрозы на ближайшее будущее:

1. Интернет вещей как площадка для реализации атак (маршрутизаторы, видеокамеры, мобильные приложения).
2. Мобильные приложения как разносчики вредоносного ПО и «воры данных».
3. Программы-вымогатели и сопутствующие им технологии.
4. Атаки «третьего поколения». Использование протокола DNS для скрытия активности ВПО, CDN, BGP.
5. Целенаправленные угрозы, реализующие полный цикл kill chain.
6. Атаки на цепочки поставок (внедрение вредоносного кода в программное обеспечение в OpenSource).
7. Кража данных известных лиц с последующим шантажом.
8. Criminal-as-a-Service.
9. «Призраки Интернета прошлого». Угрозы от устаревшего программного и программно-аппаратного обеспечения, которое находится в Интернете.
10. Нехватка людей для реализации возрастающего числа задач.

Согласно исследованию CISCO, с точки зрения реализации мер защиты Россия обходит многие государства по 9 из 11 пунктов. Одной из основных сложностей в обеспечении ИБ в России является:

- отсутствие целостного взгляда на ИБ (архитектура);
- неполный мониторинг и реагирование на инциденты (SecOps).

Многие инциденты остаются незамеченными, что приводит к последствиям по реализации негативного ущерба. Умение измерять ущерб от инцидента информационной безопасности – важный навык, которому необходимо учиться.

Другие примеры последствий угроз:

- смерть пациентов;
- падение курса акций;
- кража интеллектуальной собственности;
- снижение объема обогащенного топлива;

- влияние на результаты выборов;
- нарушение работы сети Интернет;
- блокирование дверей;
- взлом кардиостимулятора;
- отказ тормозов в автомобиле;
- атака на систему управления полетами и транспортом.

Gartner создал Gartner hype cycle (Гартнер хайп) – это кривая развития технологий, показывающая, что любая технология со временем меняется (рис. 5). Гартнер хайп состоит из этапов:

- R&D – исследования и разработки;
- хайп – все говорят о технологии, не понимая, что она из себя представляет и какую пользу несёт для бизнеса;
- время принимать решения;
- время неоправданных ожиданий;
- пилотирование;
- плато продуктивности – технология приносит прибыль.

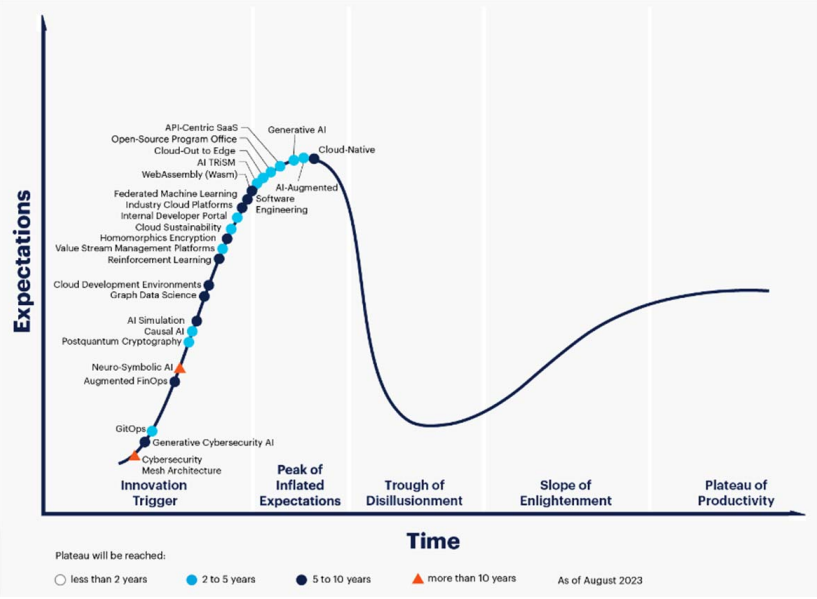


Рис. 5. Gartner hype cycle (кривая развития технологий)
https://gartner.com/en/articles/what-s-new-in-the-2023-gartner-hype-cycle-for-emerging-technologies

С помощью данной кривой можно оценивать различные решения и сегменты рынка по информационной безопасности.

Защита финтеха

В зависимости от финансовой сферы (банки, пенсионные фонды, инвестиции, страхование) будут развиваться собственные направления финтеха:

- краудфандинг;
- P2P – кредитование;
- мобильный банкинг;
- банк as-a-platform;
- алгоритмический трейдинг.

Цифровая трансформация делится на авральную (внедряем технологии внезапно) и плановую.

Новые технологии и тенденции, внедряемые в финансовые организации, невозможно рассматривать в отрыве от кибербезопасности:

1. Цифровые помощники (чат-боты, голосовые помощники).

2. Интернет вещей подключает автомобили, видеокамеры, денежные мешки, банкоматы, пропуска.

3. Облачные технологии позволяют сэкономить на материальных активах. Однако требуют обеспечения ИБ на платформе, не принадлежащей организации, с нечетким местоположением.

4. Мобильность. С целью увеличения прибыли организация направляет сотрудников как можно ближе к клиентам. Сотрудники оснащены смартфонами, ноутбуками, планшетами. Это размывает периметр, увеличивает площадь атаки и перекладывает часть задач ИБ на неопытных пользователей.

5. Программируемые сети (SDN) и отсутствие контроля за связностью в сети Интернет (BGP) открывают возможность для перехвата трафика. Например, контроль перемещения грузов и передвижения мобильных групп. С одной стороны, это возможность, с другой – угроза. На перемещаемый датчик на инкассаторском броневике можно воздействовать джаммером и тем самым блокировать передачу данных местонахождения охраняемого актива с последующей его кражей.

6. Социальные сети становятся источником распространения негативной информации о компании, а также каналом проникновения.

7. Новое рабочее место работника (динамичное, BYOD, BYOT) создает новые сложности для обеспечения ИБ.

8. Анализ больших данных приводит к нарушению законодательства о персональных данных.

9. Квантовые вычисления. Появление квантовых компьютеров ставит под вопрос текущие механизмы криптографической защиты информации, так как их можно будет легко и быстро взломать.

10. Искусственный интеллект и машинное обучение позволяют подменить результаты, по которым работает голосовой/видео помощник или чат-бот, и предпринять меры по предотвращению реализации угроз.

Переход на удаленную работу ставит задачу защиты удаленного доступа. Можно использовать решения VDI, RDP, решения по VPN. Они будут зависеть от применяемых приложений.

Защита машинного обучения также зависит от приложений, так как существуют технологии предиктивные, прогностические и аналитические. Необходимо бороться с угрозами, направленными на дата-сет. Для этого нужно разрабатывать механизмы защиты, не дожидаясь регуляторов.

С точки зрения кибербезопасности цифровой трансформации необходимо думать:

- о цифровых двойниках;
- блокчейне;
- средствах групповой работы (TrueConf, CommuniGate).

Данные решения являются приоритетными. Можно внедрять их в учебный процесс для того, чтобы при трудоустройстве молодые специалисты уже умели пользоваться новыми технологиями информационной безопасности.

Востребованные технологии на внутреннем рынке кибербезопасности

Тенденции сетевой ИБ:

1. Централизованное управление, включая смешанное (cloud + on-premise).

2. Интеграция с решениями по расследованию сетевых инцидентов.

3. Инспектирование зашифрованного трафика путем:

- расшифрования;
- работы с зашифрованным трафиком через гомоморфное шифрование или использование машинного обучения для обнаружения смыслов.

4. Микросегментация.

5. Интеграция с Threat Intelligence.

6. Переход на SaaS-модель.

7. Использование виртуальных межсетевых экранов.

8. Использование облачных межсетевых экранов с готовыми сценариями для облаков (AWS, Azure, GCP, Sber).

9. Оркестрация и автоматизация процессов, которые объединят в единую инфраструктуру безопасности множество продуктов.

10. Мониторинг аномалий. Корректнее учить аномалиям, когда они неизвестны или их сложно описать. Нужно анализировать другие виды данных (трафик, логи более объемного состава, бизнес-активность организации).

Важны виртуальные файерволы, которые умеют фильтровать трафик с уровня Л-3 до Л-7. То же самое касается шифрованного трафика, который составляет более 50–60 % от общего объема трафика. Необходимо уметь его мониторить, выявлять вредоносный код, защищать.

Инфраструктурная безопасность – наиболее проработанный зрелый рынок, а также наиболее понятный для российских компаний.

Тенденции защиты хостов:

- использование EDR решений (Gartner) или STAP (IDC). Российские вендоры (Касперский, Юзергейт) активно входят в этот сегмент;
- все в одном (шифрование, DLP, сканер);

- локальная или облачная песочница для анализа подозрительных файлов;
- интеграция с сетевыми решениями за счет обмена данными или резолюциями;
- поддержка SaaS-модели;
- решения класса NG Endpoint Security (несколько антивирусов, antimalware-движков, контроль репутации файлов, корреляция IP и URL).

Тенденции Identity & Access Management:

- управление привилегированными пользователями (PAM);
- многофакторная аутентификация;
- софт-токены, позволяющие реализовать второй фактор без дорогостоящих решений;
- биометрия;
- динамическая (контекстная) аутентификация;
- поддержка модели IdaaS;
- интеграция с другими средствами защиты (МСЭ, IPS, SIEM);
- идентификация сотрудников и клиентов;
- федеративные системы;
- контроль поведения пользователей с помощью UEBA (UBA).

UEBA, с одной стороны, относят к DLP-сегменту, а с другой – при ее разработке применяется большое количество технологий (SIEM, EDR, PAM, мониторинг утечек информации). Возможно, сегмент отдельных продуктов UEBA перестанет существовать и будет встроен в уже существующие решения (SIEM).

Тенденции DLP:

- контроль облаков и мобильных устройств;
- акцент на compliance (GDPR);
- автоматизация и простота управления;
- дополнительный мониторинг сотрудников, улучшенный workflow и управление инцидентами;
- интеграция с другими решениями по ИБ:

– средства маскирования данных;
– шифрование файлов;
– файерволы для баз данных;

– шифрование баз данных;
– решение класса DRM;
– реализация конструкций compliance as a code, позволяющих продолжать работать в области регулирования и при этом погружаться в разработку программных систем.

Тенденции мобильной ИБ:

- интеграция с инфраструктурой ИБ;
- обмен информации об угрозах (Threat Intelligence);
- поддержка SaaS-модели;
- уклон в Detection & Response (EDR / STAP);
- тенденции хостовой ИБ.

Облачные тенденции:

- активное внедрение CASB (Cloud Access Security Broker);
- смешанное управление (облачное + on-premise);
- поддержка в модели SaaS;
- переход к аутсорсингу/облачной ИБ по причине нехватки персонала;
- переход от модели MSSP к MDR (позволяет передать функцию обеспечения информационной безопасности аутсорсинговой компании).

На горизонте 1–5 лет облачные технологии будут играть важную роль. Необходимо обратить внимание, что объект защиты находится за пределами корпоративной или ведомственной сети.

Другие тенденции:

- форензика – сбор цифровых доказательств, включая облака;
- интеграция vulnerability management и решения AppSec – продукт не выпускается на рынок, если уязвимость критична (выведение решения из строя, нанесение ущерба, кража данных);
- интеграция SecOps и DevOps;
- внедрение Threat Intelligence в деятельность российских предприятий, занимающихся безопасностью;
- возврат к обманным технологиям;
- легковесная криптография – хорошо работает в электронном голосовании, интернете вещей, трейдинге бумагами, финансовой деятельности в целом;

- балканизация интернет- и мирового рынка ИБ – американский сегмент + сателлиты, европейский, китайский, латиноамериканский или южноамериканский и российский сегменты;
- аналитика и визуализация ИБ (SOC – это следствие);
- страхование киберрисков – при реализации инцидента страховая компания возмещает ущерб;
- отсутствие периметра (Zero Trust) – выстраивание защиты, исходя из парадигмы, что нас в любом случае атакуют. Надо уметь вовремя это обнаружить.

Аналитика – это обязательная функция любого продукта по информационной безопасности. Важно уделять внимание обучению аналитиков информационной безопасности. Бессмысленно учить в вузе администраторов файерволов, ВПН-решений или антивирусов. Нужно учить конструкторов, архитекторов, аналитиков информационной безопасности, тех, от кого зависит информационная безопасность, в том числе с точки зрения экономики для организации.

Средства защиты должны быть оснащены аналитикой. С ее помощью можно:

- описать, что происходит (системы обнаружения вторжений, антивирусы, SIEM);
- диагностировать, почему это происходит (NTA, UEBA, NFT, EDR);
- предсказать, что произойдет (Fraud Detection);
- предписать, что я должен сделать (Attack Simulation либо решение класса SOAR).

Особенности российского рынка

Важно понимать, как развивается российский рынок информационной безопасности.

Тенденции рынка до 24 февраля 2022 г.:

- ужесточение требований ФСТЭК к разработчикам и лицензиатам. В учебном процессе стоит применять продукты, имеющие сертификаты, а также учить студентов выбирать средства защиты с точки зрения Compliance;
- рост числа стартапов, ориентированных на западный рынок;

- соотношение иностранных решений и отечественных 3/1. Сейчас соотношение будет меняться в сторону 0/1. Следует заранее учить студентов российским решениям;
- усиление требований ФСТЭК по сертификации и снижение числа сертифицированных решений;
- рост регуляторики;
- цифровой суверенитет – импортозамещение операционных систем, баз данных, приложений, оборудования, серверов, процессоров.

С точки зрения того, на базе чего учить, у иностранных компаний большое количество решений, которые можно было внедрять в процесс обучения. У российских игроков их гораздо меньше.

Российский рынок средств защиты развит слабо и преимущественно ориентирован на регулятивные требования (наиболее развит рынок antimalware, СКЗИ/VPN, МСЭ/СОВ, DLP, SIEM). В большинстве продвинутых ниш рынка ИБ присутствует всего 1–2 игрока, что недостаточно для адекватного выбора и нормальной конкуренции. Функциональность, качество и возможность массового производства средств защиты российского производства сильно уступают зарубежным аналогам.

Тенденции в нормотворчестве:

- безопасность критической инфраструктуры;
- персональные данные;
- требования по оценке соответствия;
- усиление требований к квалификации персонала;
- согласно Указу президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», организация, подпадающая под действие Указа, должна иметь заместителя генерального директора по информационной безопасности. Данную позицию может занимать человек, имеющий высшее образование в области информационной безопасности либо прошедший профессиональную переподготовку;
- усиление контроля сети Интернет;
- геополитика;
- расширение роли Центрального банка.

С точки зрения того, чем защищаться, российский рынок информационной безопасности оценивается в 80 миллиардов рублей. Около 200 компаний разрабатывают средства защиты.

К лидерам рынка первого эшелона можно отнести Лаборатория Касперского, BI.ZONE, Positive Technologies, Ростелеком Солар.

Ко второму эшелону – Код безопасности, Инфотекс, Эшелон, Group-IB, Газинформсервис, Конфидент.

Третий эшелон – еще порядка 200 нишевых разработчиков, занимающихся разработкой 1–2 продуктов.

Не все из них выживут, так как помощь со стороны государства будет распределяться исходя из масштаба разработчика. Взаимодействовать в образовательном процессе стоит с теми, кто:

- не первый год на рынке;
- обладает финансовой подушкой;
- может поддерживать собственное развитие в условиях непростой геополитической ситуации.

20 тем кибербезопасности на повестке дня руководителя службы информационной безопасности:

1. Поддержка руководства.
2. Метрики, которые имеют значение.
3. Обоснование бюджета.
4. Фокус: подтверждение/обнаружение.
5. Оценка влияния на бизнес.
6. Раскрытие фактов утечки в паблик.
7. Взаимодействие внутри компании.
8. Тренд на аутсорсинг.
9. Подготовка к инцидентам.
10. Влияние патчей на утечку данных.
11. Причины простоев.
12. Мобильные работники.
13. Обнаружение угроз и zero trust.
14. Сетевая инфраструктура.
15. Многовендорная сложность.
16. Причины киберусталости.
17. Преимущества облаков.

18. Цифровая трансформация.
19. Усиление реагирования на инциденты.
20. Улучшение состояния ИБ.

Сегодня решения по информационной безопасности меняются. Подходы к образованию должны меняться с учетом тенденций, влияющих на рынок, а именно:

- угроз кибербезопасности;
- технологий;
- технологий кибербезопасности.

Это позволит развиваться российскому рынку информационной безопасности, образованию, технологиям и решениям.

Актуальность обеспечения кибербезопасности

Вопросы кибербезопасности становятся повседневной проблемой бизнеса. Ландшафт угроз определяется массовым уходом сотрудников на удаленную работу во время пандемии и повсеместным распространением мобильных устройств и устройств интернета вещей. Указ президента России № 250 от 1 мая 2022 г. на ближайшие годы определяет потребности кибербезопасности в российском бизнесе и государственных организациях. На состоявшемся в мае 2022 г. Всемирном экономическом форуме в Давосе отмечался рост в 2021 г. объема кибератак на 125 % по сравнению с предыдущим годом. Атаки на критическую инфраструктуру, от которой зависит повседневная жизнь большого числа людей, заставляет рассматривать современную кибербезопасность как часть ESG. Что касается России, то, по данным Лаборатории Касперского, Россия оказывается самой атакуемой страной в мире.

С марта 2022 г. интенсивность кибератак на российские организации многократно возросла. Крупные компании и рейтинговые агентства публикуют на регулярной основе обзоры по состоянию кибербезопасности. В частности, 94 % кибератак начинаются с вредоносного сообщения электронной почты. 55 % атак на крупный бизнес происходят по модели supply chain attack.

Статистика, тенденции и эволюция киберугроз

По данным апрельского обзора Gartner за 2022 г., выделяются семь мировых тенденций в кибербезопасности.

1. Расширение поверхности атаки. В связи с массовой удаленной работой во время пандемии злоумышленникам оказалось легче проникать в корпоративные сети, атакуя слабо защищенные домашние или личные устройства сотрудников, работающих удаленно.

2. Защита систем идентификации. Рабочая пара логин/пароль в руках злоумышленника является в настоящее время ключом для успешного развития кибератак. Получить ее можно разными способами. Наиболее популярным из них является фишинг.

Gartner рассматривает защиту систем идентификации как мировой тренд.

3. Риск атак на цепочки поставок имеет тенденцию к росту. Большие корпорации хорошо защищены, что делает прямые атаки нерентабельными. Однако проникновения через сети компаний-партнеров более вероятны. Поскольку уровень зрелости кибербезопасности в небольших компаниях ниже, взломать их легче, а далее использовать их сети как плацдарм для развития атаки на основную компанию.

4. Консолидация вендоров. Наблюдаемая тенденция показывает улучшение совместимости продуктов кибербезопасности от разных вендоров (на уровне стандартов, протоколов), а также интеграцию разных функций кибербезопасности в одном продукте.

5. Сеть кибербезопасности. Речь идет о реализации принципа Zero Trust. Средства безопасности интегрируются с конечными устройствами, с серверами в дата-центрах или облачных инфраструктурах. Gartner предсказывает, что к 2024 г. организации, внедрившие подобную архитектуру, смогут снизить потери от индивидуальных инцидентов кибербезопасности на 90 %.

6. Распределенное принятие решений. В больших организациях централизованная роль CISO недостаточна для принятия решений по всему объему событий кибербезопасности. Может потребоваться либо географическое распределение центров принятия решений, либо их разнесение в зависимости от экспертизы.

7. Больше, чем осведомленность. Простого обучения недостаточно для выработки у сотрудников организации устойчивых навыков кибергигиены. Пользователей необходимо тренировать.

Тенденции кибербезопасности в России следуют мировым, но имеют и отличия. Россия в настоящее время является участником кибервойны, причем атакуемой стороной. США и Украина открыто признают, что проводят «наступательные» кибератаки в отношении российских организаций. Изменился и подход к DDoS-атакам.

Пользователи по политическим мотивам добровольно включают свои устройства в сети botnet, чтобы стать участниками кибератак.

Фейковые новости активно тиражируются благодаря соцсетям. Явная дезинформация вредит бизнесу и может преследовать политические цели. Сбербанк был вынужден открыть на своем вебсайте специальную страницу для разоблачения публикуемых фейков.

Нехватка специалистов в области кибербезопасности ощущается во всем мире, но в России вопрос стоит более остро в связи с необходимостью выполнять Указ президента России № 250 от 1 мая 2022 г. В частности, большое число организаций должны создать выделенные департаменты информационной безопасности и до начала 2025 г. перейти на средства киберзащиты, разработанные в России или дружественных странах. Реализация Указа потребует привлечь дополнительно не менее 30 тыс. высококвалифицированных специалистов в области кибербезопасности.

Прекращение предоставления услуг большинством мировых удостоверяющих центров российским компаниям, по сути, означает подрыв мирового доверия в киберпространстве, поскольку именно на доверии основана инфраструктура открытых ключей. Аннулирование подписок на облачные услуги, включая подписки на функционал, относящийся к средствам безопасности, также оставляет организации открытыми перед киберугрозами. Доверие к производителям решений кибербезопасности утрачивается.

Большинство успешных кибератак и утечек конфиденциальной информации происходит из-за человеческих ошибок, а не из-за уязвимостей в информационных системах. Но если человеческие ошибки имеют поведенческие решения, то технологические уязвимости можно исправить лишь установкой исправлений ПО.

В декабре 2021 г. была обнаружена критическая уязвимость Log4Shell в очень популярной JAVA-библиотеке. Она затрагивает сотни миллионов экземпляров веб-серверов Apache, дает возможность выполнить на веб-сервере произвольный код с административными правами, а проэксплуатировать уязвимость могут даже начинающие хакеры. Уязвимость в открытом исходном коде (open source) оставалась незамеченной с 2013 г. Уязвимость Log4Shell считается одной из самых серьезных найденных уязвимостей за всю историю, и даже сейчас она остается незакрытой на многих веб-серверах.

Другой тенденцией остается взлом устройств интернета вещей (IoT) для организации дальнейших кибератак. Устройства IoT в большинстве своем обладают лишь базовыми средствами безопасности. Их ПО не обновляется или обновляется нерегулярно. К ним невозможно применить накладные средства защиты. Все эти недостатки эксплуатируются злоумышленниками. Именно так развивались события с роутерами Mikrotik, в которых firmware не последней версии оказалось уязвимо. В результате злоумышленники получили контроль над 250 тыс. устройств IoT и использовали их в мощнейшей DDoS-атаке на Yandex в сентябре 2021 г.

Для защиты инфраструктур с использованием устройств IoT необходимо выделять последние в отдельные IP-подсети с контролем трафика. Но самым эффективным методом защиты является поведенческий анализ сетевого трафика от устройств IoT с использованием моделей машинного обучения.

Вирусы-шифровальщики громко заявили о себе в 2017 г. эпидемиями WannaCry, Petya, NotPetya. Однако и в 2021 г. наблюдается двукратный рост атак, предпринимаемых вирусами-шифровальщиками. Так, успешная атака в мае 2021 г. на американскую компанию Colonial Pipeline, обеспечивающую перекачку нефтепродуктов по всей территории США, привела к тому, что работа компании была парализована и компания была вынуждена заплатить злоумышленникам выкуп. В результате нарушения снабжения топливом аэропорта в Атланте пришлось перестраивать множество авиарейсов. Дальнемагистральные рейсы выполнялись с промежуточными посадками для дозаправки.

Для распространения по сети вирусы-шифровальщики используют общеизвестные критические уязвимости. Широкое распространение получила модель ***Ransomware as a Service***, когда злоумышленник может не разрабатывать собственный вирус-шифровальщик, а «арендовать» стороннее вредоносное ПО для организации собственной кибератаки.

Другая тенденция получила наименование ***double extortion ransomware***. В последнее время перед шифрованием предпринимается попытка скопировать из сети организации конфиденциальную информацию с целью двойного шантажа. Компания не вернет зашифрованную информацию, если не заплатит выкуп, и по этой же причине злоумышленники угрожают опубликовать конфиденциальную информацию компании или продать ее всем, кого она заинтересует.

За исторически короткий период в 40 лет кибератаки совершили гигантский скачок. От простого угадывания паролей до deepfake – почти не отличимой цифровой копии личности со звуком и видео. Кибератаки стали доступными как по бюджету, так и по требуемым компетенциям.

Ряд компаний (Radware, Лаборатория Касперского, CheckPoint, SpamHaus), предлагающих решения в области кибербезопасности, поддерживают на своих сайтах онлайн-визуализации, показывающие кибератаки, которые происходят в реальном времени. В качестве поставщиков данных выступает антивирусное ПО на конечных устройствах, сетевое оборудование и т. д.

Успехи и достижения кибербезопасности

В начале 2022 г. решения Сбербанка в области кибербезопасности получили престижные золотые и серебряные европейские награды в 7 номинациях. Борьба со спамом – мировой успех кибербезопасности.

На рубеже нулевых и десятых годов объем спама в мировом трафике электронной почты достигал 90 %. Однако в настоящее время его доля снизилась более чем в 3 раза. Это не победа, но очевидный перелом ситуации, и он стал возможным благодаря внедрению эффективных антиспам-фильтров на основе моделей машинного

обучения. Решение, когда модель обучается на заранее классифицированном большом наборе электронных писем, а затем приступает к обработке реального потока, оказалось эффективным с малым числом ложных срабатываний. Другой успех – финансовые антифрод-системы и, в частности, антифрод в Сбербанке.

Эффективная борьба с кибермошенничеством позволяет России находиться в числе стран с самым высоким уровнем предоставления финансовых услуг через Интернет. В антифрод-систему Сбербанка стекается информация о финансовых транзакциях по всем возможным каналам обслуживания.

В анализе задействовано около 100 моделей на основе искусственного интеллекта. Платежная система дает лишь порядка 100 мс на принятие одного из решений: разрешить финансовую транзакцию, отклонить ее или направить на дополнительную аутентификацию.

Рабочие модели в антифроде включают:

- скоринги сущностей: оценивают клиентов и их устройства, участвующие в финансовой транзакции, на основании их «поведения» в прошлом и по другим аспектам;
- гео-модели: выявляют нетипичные перемещения участников финансовой транзакции;
- графовые: строят финансовые связи между клиентами, устройствами, оценивают их финансовую близость, эффективны при выявлении мошеннических групп.

Еще одно достижение, которым предстоит воспользоваться в ближайшем будущем, относится к области криптографии. Современные асимметричные криптографические алгоритмы демонстрируют свою устойчивость и применяются повсеместно – от больших серверов до мобильных устройств. Но так будет не всегда. Уже доказано, что асимметричный шифр можно взломать за разумное время на квантовом компьютере. Пока не существует квантовых компьютеров требуемой мощности, но ожидается, что они будут созданы в течение ближайших 10 лет.

После этого современные и используемые повсюду асимметричные криптографические алгоритмы больше не будут считаться стойкими. Одно из решений состоит в безопасной передаче симме-

тричного ключа шифрования (именно он шифруется на открытом ключе в асимметричной криптографии) благодаря не математике, а на основе физических принципов, а именно квантово-механических свойств фотонов. Соответствующий протокол был разработан еще в 1984 г. Такой подход уже прошел экспериментальную проверку, и в 2021 г. в России, между Москвой и Санкт-Петербургом, заработала первая линия оптоволоконной связи с полностью квантовой передачей симметричного ключа.

Атака как сервис

Среди мотивов кибератакующих с явным преимуществом лидирует финансовый. Хакерам либо платят за их работу, либо они, как в случаях с вирусами-шифровальщиками, требуют выкуп. Инсайдеры также должны оставаться в центре внимания, поскольку, будучи сотрудниками, они уже имеют доступ к информационным ресурсам организации. Они могут действовать как со злым умыслом, так и по незнанию.

Третью строчку занимают, как правило, начинающие хакеры, для которых взлом – способ повысить самооценку и авторитет в сообществе. Хакерские группы, выполняющие государственные заказы, уже не являются тайной в условиях развязанной кибервойны и занимают четвертое место в рейтинге. Их не следует смешивать с группами, действующими в политических интересах. Причем их политические цели могут время от времени меняться. Наиболее известными такими группами до недавнего времени была Wikileaks, сейчас – Anonymous. Их еще называют хактивистами, однако к последним также относятся добровольные специалисты по безопасности, которые находят уязвимости безопасности в сетях больших организаций и конфиденциально сообщают о своей находке. При этом они дают срок на устранение и по истечении этого срока, независимо от того, устранена ли уязвимость, публикуют о ней информацию в открытых источниках. У организации не остается выхода, как своевременно устранить уязвимость и повысить свою безопасность.

Существует и иная мотивация, но она менее распространена. Чтобы организовать кибератаку, не требуются специальные знания или значительный бюджет. Кибератаку заказать очень просто.

Для этого не нужно искать исполнителя в даркнете. С помощью обычной поисковой системы легко найти предложения услуг, чтобы, например, организовать DDoS-атаку на сайт конкурирующей фирмы. Рынок киберпреступности очень хорошо организован. Он не зависит от национальных законодательств, границ и таможен.

Различные механизмы генерации прибылей, собственные всеми признаваемые валюты (криптовалюты), хакерские форумы как торговые площадки, где можно договориться об услуге, посмотреть предложения о работе в хакерской группе или разместить свое предложение, найти инсайдера в выбранной компании, обучиться инструментарию злоумышленников или получить техническую поддержку. Есть даже штатные психологи, разрабатывающие новые сценарии социальной инженерии.

Модель Kill Chain

Для описания кибератак и злоумышленников в кибербезопасности применяются различные модели.

Мы рассмотрим популярную модель **Cyber Kill Chain** – модель многоступенчатой развивающейся во времени кибератаки. Она содержит 7 шагов и дополнительный – уничтожение следов.

На первом шаге – **разведке** – злоумышленник использует открытые источники для сбора подробной информации об атакуемой компании: адреса электронной почты, технические заголовки писем, веб-сайт организации, данные WhoIs, сканирование портов узлов компании в Интернете. На основании собранной информации разрабатывается план кибератаки.

На втором шаге – **вооружении** – злоумышленник пишет самостоятельно или заказывает разработку вредоносного кода и планирует его доставку. Также может использоваться стандартный инструментарий.

На третьем шаге происходит **доставка**. Самым популярным способом доставки является фишинг.

Если вредоносный код удалось запустить, то атака развивается и переходит на четвертый шаг – **проникновение**.

На шаге **инсталляции** запущенное вредоносное ПО дозагружает недостающие компоненты – они могут составлять значительный

объем. Предпринимаются усилия по повышению привилегий в системе. Не исключено, что будет сформирован канал коммуникации с центром управления злоумышленника.

На шаге **управления** злоумышленник получает информацию изнутри атакуемой информационной системы, контроль над новыми компьютерами или иными устройствами, т. е. изучает внутреннее устройство системы и горизонтально расширяет атаку.

Если злоумышленник не обнаружен, он переходит к **реализации** целей. Это может быть выведение из строя инфраструктуры, хищение конфиденциальной информации, шифрование данных с требованием выкупа.

Если цель атакующего достигнута и он до сих пор не обнаружен, то злоумышленник уходит, **уничтожая** за собой логи и иные **следы**, которые могут выдать его присутствие и помочь расследованию.

По модели Kill Chain в качестве примера расписана атака на British Airways, которая произошла в 2018 г. Персональные данные почти 400 тыс. клиентов, приобретавших билеты на сайте British Airways, включая данные банковских карт, утекли к злоумышленникам.

Это также пример атаки на цепочку поставок, когда атаке подвергся веб-сайт компании-партнера (через нее проходила финансовая транзакция), а пострадала основная компания. Путем сканирования портов хакеры обнаружили уязвимость на веб-сайте и разработали, а затем разместили на сайте вредоносный скрипт, похищающий персональные данные клиентов. Информация отправлялась на созданный злоумышленниками веб-узел с именем, созвучным с наименованием авиакомпании, но не имеющий к ней никакого отношения. Злоумышленники даже получили для него публичный сертификат.

Современные парадигмы кибербезопасности

В октябрьском обзоре Microsoft за 2021 г. перечислены современные парадигмы кибербезопасности. Кибербезопасность в настоящее время рассматривается как часть устойчивости бизнеса. Важнейшей парадигмой считается цифровая гигиена. От навыков сотрудников использовать сложные и разные пароли, противосто-

ять фишингу и социальной инженерии зависит предотвращение кибератак на начальной стадии.

Кроме того, в настоящее время риски кибербезопасности должны рассматриваться как часть бизнес-рисков, и все принимаемые решения должны расцениваться с точки зрения кибербезопасности.

Средства кибербезопасности должны выполнять свои функции, но в то же время не мешать основной работе. Более того, следует стремиться к комфортной и дружелюбной рабочей среде, чтобы стандартные операции, связанные с кибербезопасностью, например, смена пароля, сброс забытого пароля, были удобны, понятны и не приводили пользователя в состояние растерянности.

Контрольные вопросы

1. Какое утверждение соответствует тренду развития рынка ИБ-специалистов в России на ближайшие годы?
2. Какое утверждение соответствует тренду развития мирового хакерского рынка?
3. Какие из перечисленных киберугроз являются ключевыми на ближайшее будущее?
4. Что является тенденциями сетевой информационной безопасности?
5. Что является тенденциями хостовой информационной безопасности?

Тесты для самоконтроля

1. Что из нижеперечисленного является тенденциями Identity & Access Management? Выберите все правильные ответы.

а) более эффективное управление привилегированными пользователями
б) внедрение однофакторной аутентификации
в) отказ от использования софт-токенов в пользу биометрии
г) интеграция со средствами защиты IPS и SIEM
д) контроль поведения пользователей с помощью технологии UEBA
е) внедрение локальной аутентификации

2. Что из нижеперечисленного относится к трендам развития процесса DLP? Выберите все правильные ответы.

а) контроль облаков и мобильных устройств

б) акцент на compliance

в) шифрование данных

г) контроль Big Data

д) внедрение процесса DevSecOps

е) управление на основе API

3. Какой способ начала кибератаки самый распространенный в настоящее время?

а) подбор пароля по словарю

б) фишинг

в) сканирование портов

г) перехват сетевого трафика

4. В чем особенность кибератак с применением вирусов-шифровальщиков начиная с 2020 года?

а) выкуп для расшифрования данных запрашивается неоднократно

б) не всегда удается расшифровать данные

в) перед шифрованием предпринимается попытка похитить конфиденциальную информацию

г) вирус-шифровальщик распространяется по сети, используя незакрытые уязвимости

5. Какой подход наиболее эффективен в обеспечении кибербезопасности устройств интернета вещей?

а) установка антивируса на устройства IoT

б) физическая безопасность

в) назначение сложных паролей

г) поведенческий анализ на основе моделей машинного обучения

Тема 3. УПРАВЛЕНИЕ ДАННЫМИ КИБЕРБЕЗОПАСНОСТИ

Форма проведения занятия – лекция.

Вопросы для обсуждения

1. Какие требования с точки зрения ИБ к шине данных (Kafka)?
2. С какими основными проблемами по управлению данными сталкиваются организации и как пытаются их решить?

Методические указания по проведению занятия

При освоении темы необходимо:

1. Изучить учебный материал по теме 3.
2. Акцентировать внимание на основополагающих понятиях и определениях.
3. Ответить на контрольные вопросы по теме 3.
4. Выполнить тест по теме 3.

Методическое оборудование к занятию: проектор, ноутбук.

Рекомендуемая литература

1. Кийко, П. В. Цифровые технологии : учеб. пособие / П. В. Кийко ; Омский государственный аграрный университет имени П.А. Столыпина. – Омск : ФГБОУ ВО Омский ГАУ, 2023. – 108 с. – URL: e.lanbook.com/book/349799 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-907687-34-9.
2. Надёжность и защита информации автоматизированных систем : учеб. пособие / М. Н. Краснянский, В. Г. Матвейкин, А. В. Затонский [и др.] ; Тамбовский государственный технический университет. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2022. – 95 с. – URL: e.lanbook.com/book/355145 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8265-2460-2.

Краткие теоретические сведения

Data Governance – это набор практик, процессов, методологий, обеспечивающих управление информационными активами внутри организации. На сегодняшний день включает 10 доменов:

1. Архитектура данных.
2. Метаданные.
3. Моделирование и проектирование данных.
4. Справочные и основные данные.
5. Безопасность данных.
6. Интеграция данных.
7. Управление документами и контентом.
8. Хранение и операции с данными.
9. Хранилища данных и бизнес-аналитика.
10 Качество данных. Их цель – извлечение пользы из данных организации.

С устройств платформ Сбера и внешних систем собираются и обрабатываются более 350 млрд событий в сутки:

- телеметрия от сетевых устройств и устройств защиты;
- системные логи и журналы;
- аудит серверов и рабочих станций;
- данные из инфраструктуры и информационных систем;
- внешние источники информации об уязвимостях;
- транзакционная активность клиентов.

Без выстраивания процессов управления данными невозможно реагировать на угрозы и события кибербезопасности.

Сегодня в платформах Сбера используются данные кибербезопасности:

- для построения аналитических витрин с последующей передачей во внутренние и внешние системы;
- внедрения в различные бизнес-процессы (уже более шести подразделений используют данные кибербезопасности в своих бизнес-процессах);
- расчета скорингов и обучения моделей выявления мошенничества и киберугроз;

- создания собственных аналитических продуктов на платформе кибербезопасности;
- моделирования и исследования по данным кибербезопасности на основе созданного Data Lake.

Управление жизненным циклом

Экспоненциальный рост данных кибербезопасности привел к большой утилизации ресурсов и определил процесс управления жизненным циклом данных одним из важных для Сбербанка в управлении данными.

Выделяется девять этапов жизненного цикла данных:

1. Определение данных.
2. Сбор данных.
3. Описание данных.
4 – 6. Обработка, транспорт и хранение данных.
7. Использование данных.
8. Формирование отчетности.
9. Определение политики хранения и уничтожения данных.

Пример архитектуры этапов жизненного цикла в Сбербанке

Какие данные собираются в Сбербанке?

- системные логи и журналы аудита серверов и конечных устройств;
- телеметрии от сетевого оборудования и устройств безопасности по периметру;
- транзакционные данные от клиентов;
- данные об инфраструктуре;
- информационные сервисы;
- справочная информация из автоматизированных банковских систем (видео, фото, аудио документов, которые требуется обрабатывать);
- информация из внешних источников.

Эти данные можно разделить на три группы:

- слабоструктурированные;
- структурированные;
- неструктурированные.

Для каждого типа данных определяются свои инструменты сбора (файловые обработчики, стриминговые инструменты).

После этапа сбора и преобразования данные попадают в интеграционный слой – в нашей архитектуре это интеграционная шина Kafka.

Далее этап обработки реализован по лямбда-архитектуре:

- первый слой обрабатывает события в режиме реального времени;
- второй накапливает и хранит информацию.

Долговременное хранение производится в едином Data Lake:

- аналитический слой для поиска или использования информации. Работа с данными осуществляется как специалистами (руководители, аналитики, форензик-инженеры, Data Scientists), так и в автоматизированных системах (антифрод-системы, IT и бизнес-системы платформы банка). В качестве дополнительных компонентов и инструментов управления данными используются:
- система управления метаданными или каталог моделей данных;
- аналитический поиск;
- инструменты защиты данных и безопасности;
- инструменты мониторинга и качества данных.

Работа с данными для понимания данных. Необходимо:

1. Организовать описание и связывание данных в логическую модель за счет загрузки физических данных, как базового технического слоя, и формирования бизнес-глоссария по предметным областям.

2. Выполнить маппинг терминов и понятий на физическую модель. Таким образом, создается логическая модель данных, позволяющая корректно работать с данными и получать от них пользу. Понимание данных пользователями достигается за счет поиска и анализа метаданных. Они позволяют получить следующую информацию или характеристики по данным:

- владелец данных;
- политика хранения и уничтожения данных;
- уровень критичности информации;
- уровни доступа;
- где применяются модели данных в прикладных сервисах и продуктах.

Система управления метаданными – базовый сервис, позволяющий реализовывать потребности пользователей в работе с данны-

ми, а также объединять данные и строить логическую модель организации.

Аналитический поиск по данным – важная составляющая в оперативной работе по разбору инцидентов и проведению проверок (рис. 6).

Рис. 6. Аналитический поиск по данным

Поиск должен обладать простым интерфейсом и не требовать специализированных навыков. Особенности организации сервиса поиска:

1. Поиск организуется по логической модели данных. Сервис поиска должен быть гетерогенным, то есть позволять искать одновременно по всем хранилищам данных.

2. Большой объем данных требует определенных навыков в построении поисковых систем и включает требования по количеству и разнообразию источников, объемам данных и нагрузке.

3. Отсутствие готовых решений для работы с большими данными требует использования OpenSource и разработки собственных сервисов. При небольших объемах данных потребности можно закрыть, например, с помощью Elastic и доработки управления доступом к нему.

Elastic – OpenSource – продукт, который предоставляет полнотекстовый поиск информации и позволяет реализовывать аналитический поиск.

4. Повышенные требования к информационной безопасности и доступу к данным:

- контроль доступа;
- журналирование;
- аудит;
- мониторинг обращений и поисковых запросов.

Подсистема мониторинга должна обеспечивать комплексный охват метрик и параметров в режиме «360 градусов».

Покрытие метрик, достаточное для выявления отклонений на всех уровнях работы с данными. Подсистема должна включать мониторинг:

- инфраструктурный;
- прикладной;
- бизнес-мониторинг.

Система мониторинга и качества данных Сбербанка реализована следующим образом:

1. Инфраструктурный мониторинг и мониторинг приложений покрываются централизованной банковской системой мониторинга.

1.1. На уровне инфраструктурного мониторинга собираются метрики: как работает оборудование, программное обеспечение. Под мониторингом находятся облачная инфраструктура и железные серверы, предоставляющие метрики по утилизации процессоров, памяти, жестких дисков.

1.2. На уровне мониторинга приложений отслеживаются метрики, позволяющие видеть, каким образом работают наши разрабатываемые прикладные компоненты.

2. На уровне прикладных продуктов кибербезопасности осуществляется мониторинг бизнес-метрик.

3. Мониторинг качества данных осуществляется на всех уровнях:

3.1. На уровне инфраструктурного мониторинга и системного программного обеспечения производится сбор метрик гарантированной доставки и хранения данных.

3.2. На уровне бизнес-метрик проверяется, какие данные доставляются и не утеряна ли значимая информация.

К возможным внутренним нарушителям в Сбербанке относятся:

- сотрудники банка, работающие с платформой, системные администраторы, имеющие расширенные права;
- разработчики (могут добавить в разрабатываемый код ошибки, использовать открытый код и библиотеки, содержащие уязвимости);
- Data Scientists, аналитики, имеющие доступ к критичной информации. К внешним нарушителям относятся экстремистские преступные группировки (физические лица, кибервойска).

На рис. 7 представлена модель нарушителя, необходимая для понимания основных внешних и внутренних нарушителей банковского сектора.

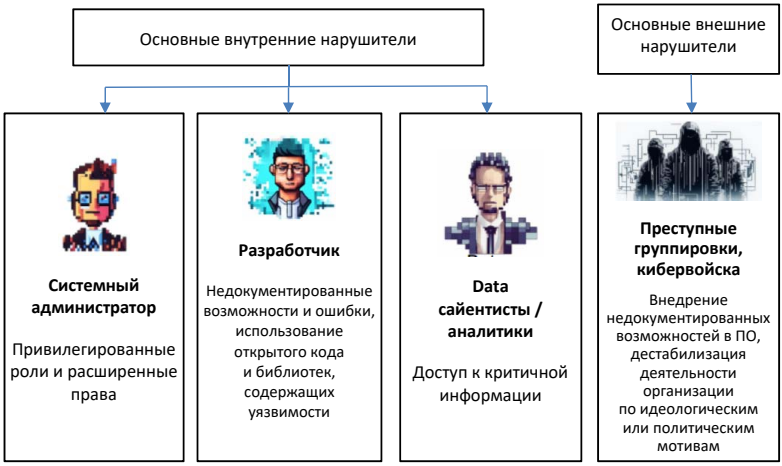


Рис. 7. Защита данных и безопасность. Модель нарушителя

Они способны внедрить дополнительные функциональные возможности в коммерческие и OpenSource-продукты.

Модель рисков и угроз Сбербанка состоит из следующих групп рисков:

- утечки/хищения конфиденциальной информации;
- нарушения целостности активов;
- нарушения управлением доступом;
- полной/частичной потери или недоступности объектов защиты;

- несоблюдения требований регуляторов. Наибольшая критичность присвоена группам рисков, связанным с утечкой конфиденциальной информации или нарушением целостности активов.

Данные риски связаны с возможностью реализации угроз:

- несанкционированный доступ к данным;
- атаки на уязвимости ПО OpenSource;
- заражение вредоносным ПО;
- компрометация учетных записей и администраторов или пользователей технических учетных записей, привилегированных пользователей;
- несанкционированные изменения, удаления конфигурации, файлов, баз данных или логов;
- ошибки и закладки при разработке ПО.

Для устранения или смягчения угроз используются механизмы:

1. Ролевая модель доступа для управления полномочиями всех пользователей платформы.

2. Pam-система для контроля действий администраторов и привилегированных пользователей.

3. Виртуальные рабочие места для Data Scientists без возможности выгрузки данных.

4. Инструменты DevSecOps (статическое тестирование, сканирование пакетов OpenSource, Quality Gates в конвейерах DevOps при сборке дистрибутивов).

Дополнительно для Data Scientists развертываются лаборатории, в которые выгружается информация, необходимая для специализированных исследований, без доступа к общему хранилищу. На всех узлах применяется шифрование каналов связи со взаимной аутентификацией сервисов, ведется сбор аудита с компонентов.

Для контроля уязвимости применяется сканер уязвимости, а результаты работы используются при планировании процесса патч-менеджмента серверов.

Для практической оценки защищенности проводятся внутренние пентесты и киберучения.

Примеры типичных уязвимостей:

1. OpenSource-компоненты, обладающие уязвимостью в компонентах за счет отсутствия механизмов аутентификации.

2. Присутствие избыточных прав, позволяющих повысить привилегии.

3. Наличие в компонентах не заблокированных стандартных учетных записей.

4. Отсутствие парольных политик, как следствие – слабый пароль учетной записи. Наличие паролей в открытом виде в конфигурационных файлах, скриптах.

5. Наличие излишних прав доступа к директориям, отсутствие политик ограничения доступа на уровне хостов. Также в Сбербанке реализован стандарт, позволяющий оценить уровень защищенности любой автоматизированной системы банка. Для руководителей – это анкета уровня защиты их систем.

Интегральный уровень поделен на стримы:

- правила;
- процессы;
- технологии.

Каждый стрим обладает критериями, весом, описанием, точной формулировкой и оценкой выполнения критерия. В сумме получается интегральный уровень защищенности автоматизированной системы.

Управление данными позволяет организации становиться Data-Driven и принимать решение, опираясь на анализ данных. Это позволяет расширить применение инструментов машинного обучения и искусственного интеллекта в кибербезопасности.

Эволюция работы с данными

Эволюция работы с данными в Сбербанке:

- сбор;
- обработка и хранение данных;
- прикладная аналитика;
- потоковый сбор, переход в режим реального времени;
- продвинутая аналитика;
- прогнозная аналитика и дополненная аналитика (ML и AI).

Контрольные вопросы

1. Какие существуют типы источников данных?
2. Какие компоненты системы аналитического поиска отвечают за доступ пользователей к данным?
3. Какой механизм отвечает за защиту учетной записи администратора от компрометации?
4. Какую опасность представляют OpenSource-библиотеки и инструменты в корпоративной среде?

Тесты для самоконтроля

1. Какой тип источников данных относится к слабоструктурированным? Выберите все правильные ответы.

а) базы данных
б) потоковые данные (json-сообщения)
в) XML-файлы
г) ETL-выгрузки

2. Какие компоненты системы аналитического поиска отвечают за доступ пользователей к данным?

а) UI + API
б) сбор
в) хранение
г) корреляция

3. Какой механизм отвечает за защиту учетной записи администратора от компрометации?

а) ролевая модель доступа
б) шифрование/токенизация
в) сетевое зонирование
г) PAM

4. Какую опасность представляют OpenSource-библиотеки и инструменты в корпоративной среде? Выберите все правильные ответы.

а) часто отсутствуют механизмы аутентификации
б) присутствуют избыточные права и повышение привилегий
в) используются нестандартные сетевые протоколы
г) встречаются незаблокированные стандартные учетные записи

д) не допускается сканирование антивирусом
е) в конфигурационных файлах встречаются пароли в открытом виде

5. Продолжите утверждение: главный постулат DATA-DRIVEN состоит в том, что решения нужно принимать, опираясь
а) на анализ данных, а не интуицию и личный опыт
б) результаты анализа AI
в) усредненную экспертную оценку
г) результаты статистических исследований

Тема 4. ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ

Форма проведения занятия – лекция.

Вопросы для обсуждения

1. Инструменты защиты (и самозащиты) искусственного интеллекта от киберугроз.
2. Насколько безопасно применять искусственный интеллект в случаях массовых атак?
3. Анализ сетевой безопасности и инфраструктуры с применением технологий искусственного интеллекта.

Методические указания по проведению занятия

При освоении темы необходимо:

1. Изучить учебный материал по теме 4.
2. Акцентировать внимание на основополагающих понятиях и определениях.
3. Ответить на контрольные вопросы по теме 4.
4. Выполнить тест по теме 4.

Методическое оборудование к занятию: проектор, ноутбук.

Рекомендуемая литература

1. Журавлёва, Н. А. Экономическая безопасность : учеб. пособие / Н. А. Журавлёва ; Петербургский государственный университет путей сообщения Императора Александра I. – Санкт-Петербург : ФГБОУ ВО ПГУПС, 2022. – 78 с. – URL: e.lanbook.com/book/224522 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-7641-1682-2.
2. Краковский, Ю. М. Методы защиты информации : учеб. пособие / Ю. М. Краковский. – Изд. 3-е, перераб. – Санкт-Петербург [и др.] : Лань, 2021. – 234 с. – URL: e.lanbook.com/book/156401 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8114-5632-1.
3. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности / Н. Ш. Козлова, N. S. Kozlova, В. А. Довгаль, V. A. Dovgal // Вестник Адыгейского государствен-

ного университета. Серия 4: Естественно-математические и технические науки. – 2023. – № 3 (326). – С. 65-72. – ISSN 2410-3225. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/journal/issue/347516 (дата обращения: 24.01.2024). – Режим доступа: для авториз. пользователей.
4. AI-Russia : открытая библиотека кейсов и премия в области бизнес-эффективности проектов, созданных с использованием искусственного интеллекта : [сайт] / Альянс в сфере искусственного интеллекта. – URL: ai-russia.ru (дата обращения: 24.01.2024).

Краткие теоретические сведения

Искусственный интеллект (ИИ) помогает решать задачи машинного обучения (ML).

Основная задача машинного обучения – разработка алгоритма, который работает с данными для принятия каких-либо решений.

ИИ – свойство интеллектуальных систем – выполнять творческие функции, которые традиционно считаются прерогативой человека.

ML – класс методов ИИ, характерной чертой которых является не прямое решение задач, а обучение за счет применения решений множества сходных задач. Ключевое отличие разработки моделей машинного обучения и систем принятия решений от традиционной разработки программного обеспечения в том, что человек не закладывает определенную логику и не реализует ее в программе принятия решений. Вместо этого используются алгоритмы, которые на основании данных строят деревья решений и решающие поверхности многомерных пространств. То есть после подачи на вход в систему новых данных уже сами алгоритмы выносят вердикты на основании виденных ими ранее данных, использованных для обучения. Человек не влияет на принятие решения. Он влияет только на подбор примеров, на которых алгоритм обучается, а также алгоритмов, которые должны будут решать задачи.

Машинное обучение находится на вершине пирамиды эволюции обработки данных. Но для качественного решения задач модели необходимо обеспечить релевантными и регулярно поступающими данными.

На сегодняшний день известно четыре класса задач машинного обучения:

1. Обучение с учителем:

- классификация нового объекта: есть массив данных, описания для отнесения к тому или иному классу и сами классы. В модель подаются новые объекты с их описаниями, модель определяет, к какому классу относится объект;
- регрессия: предсказание числового значения, числовая оценка чего-либо в зависимости от различных условий.

2. Обучение без учителя:

- кластеризация: разделение объектов массива данных на кластеры с выявлением особенностей каждого, чтобы вести более точечную работу с ними;
- поиск аномалий в данных: сначала строится модель нормальности данных, затем выявляются отклонения и проводится дополнительный анализ.

3. Обучение с частичным привлечением учителя: под имеющийся большой массив данных есть правила разметки только для части данных. В этом случае применяются специальные алгоритмы, которые пытаются разметить остальные данные.

4. Обучение с подкреплением: машина с ИИ автоматически учится в среде взаимодействия, соблюдая определенные правила. В кибербезопасности чаще всего возникают задачи обучения с учителем и в меньшей степени задачи кластеризации и поиска аномалий.

Если применение ИИ изобразить на координатной плоскости, то на одной оси будет класс задачи и используемый алгоритм, на другой – характеристики массива данных.

Выделяют две категории данных:

- структурированные: можно естественным образом представить в виде таблицы в базе данных, каждый элемент данных обладает общей структурой (например, транзакции клиентов, сетевой трафик);
- неструктурированные: каждый элемент данных уникален (например, видеоизображение, картинки, текст, запись голоса).

Сбербанк в вопросах кибербезопасности чаще всего работает с неструктурированными данными (документы в форматах .pdf, .doc,

почтовая переписка, изображения). Таким образом, при решении задач в машинном обучении необходимо определить класс задачи и категорию данных. Исходя из этого выбираются алгоритмы и подходы.

Ключевые области применения ИИ в кибербезопасности:

- противодействие мошенничеству, антифрод: оценка риска транзакций (насколько операция может быть мошеннической, а клиент – мошенником);
- расследования: по уже известным или предотвращенным случаям мошенничества выявляются дополнительные связи мошенников;
- киберзащита: выявление аномалий, заражений хостов, DDos-атак, их предотвращение, выявление фишинговых доменов;
- контроль конфиденциальной информации: нельзя допустить, чтобы информация, содержащая банковскую или коммерческую тайну, переместилась за периметр обработки либо попала в домены, где ее не должно быть.

Для противодействия социальной инженерии используются схожие модели ИИ, что и для противодействия мошенничеству в целом, но они изучают другие признаки операций. Зрелость OpenSource ML-библиотек/инструментов позволяет использовать готовый продукт для решения сложных практических задач.

Текущие data science-технологии построены на OpenSource-решениях, эффективных для разработки моделей машинного обучения. Рынок OpenSource-решений активно развивается благодаря тому, что промышленные корпорации публикуют внутренние инструменты, а сообщество разработчиков совершенствует их. Алгоритм дерева решений в рамках структурированных данных построен на том, что каждому классу объектов присваивается область определенных признаков. Например, обычный клиент получает денежные переводы, 70 % из них тратит на покупки, 20 % – переводит, 10 % – копит. Мошенник постоянно получает деньги из неизвестных источников и тут же переводит их другим.

Дерево решений:

- делит область признаков на площади;
- относит экземпляры данных объекта к тому или иному классу на основании построенной области;

- определяет, сколько признаков представляют тот или иной класс;
- перебирает доступные атрибуты;
- ищет сплиты (точки разделения по данным) с использованием математических функций оптимизации.

Путь в дереве – соответствие правилам: если признак меньше какого-то значения, идем по одной ветке, если больше – по другой. Таким образом, приходим в «листы деревьев», где есть представители классов.

Деревья решений – простой и интерпретируемый алгоритм, поскольку всегда есть правило, почему дерево отнесло экземпляр данных к одному или другому классу.

Главный недостаток алгоритма – невозможность описать сложные зависимости данных только с помощью запоминания примеров, что вытекает в «переобучение» алгоритма. Сталкиваясь с новыми данными, он дает плохой результат. Следующий этап развития обработки структурированных данных предусматривает построение не одного дерева, а ансамбля деревьев – «леса» решений – алгоритм Random forest (случайный лес).

Его принцип работы – обучающая выборка с помощью сэмплирований с возвращением делится на подмножества известных кейсов и доступных признаков. На каждом из подмножеств строится дерево решений. Деревья строятся не глубокими, а по принципу weak learns – слабыми с точки зрения принятия решения. Так как они неглубокие, не подвергаются переобучению, а строится их много, то итоговый алгоритм усредняет их предсказания о принадлежности к классу. На основании этого принимает решение.

Алгоритм Random forest достаточно устойчив к переобучению и позволяет описывать сложные закономерности, так как процессы проходят параллельно.

Контрольные вопросы

1. Какая комбинация подходов используется для обнаружения фишинговых сайтов с помощью методов AI?
2. Что такое антифрод?
3. Какой алгоритм использует AI в антифроде?
4. Какие существуют алгоритмы AI?

Тесты для самоконтроля

1. Что служит главным активом для создания решений на основе AI в области кибербезопасности?

а) структурированные данные

б) цифровые следы всех процессов

в) потоковая информация в реальном времени

г) алгоритмы

2. Какая технология AI позволила совершить качественный прорыв в обработке текстов?

а) Bag of words

б) TF-IDF

в) Transformers

г) Logistic Regression

3. Каков уровень зрелости OpenSource инструментов ML в антифроде?

а) позволяют «из коробки» решать сложные практические задачи

б) можно использовать в масштабных задачах, но требуется существенная доработка

в) подходят для решения только простых задач

г) применяются только как компонент в коммерческих решениях

Тема 5. СОВРЕМЕННЫЙ SOC

Форма проведения занятия – лекция.

Вопросы для обсуждения

1. Какое количество человек в соответствии с обязанностями должно быть в сменах SOC?
2. Какой базовый уровень развития SOC?
3. Перспективы развития SOC в решении задач кибербезопасности.

Методические указания по проведению занятия

При освоении темы необходимо:

1. Изучить учебный материал по теме 5.
2. Акцентировать внимание на основополагающих понятиях и определениях.
3. Ответить на контрольные вопросы по теме 5.
4. Выполнить тест по теме 5.

Методическое оборудование к занятию: проектор, ноутбук.

Рекомендуемая литература

1. Журавлёва, Н. А. Экономическая безопасность : учеб. пособие / Н. А. Журавлёва ; Петербургский государственный университет путей сообщения Императора Александра I. – Санкт-Петербург : ФГБОУ ВО ПГУПС, 2022. – 78 с. – URL: e.lanbook.com/book/224522 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-7641-1682-2.
2. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. – Пермь : ПНИПУ, 2023. – 91 с. – ISBN 978-5-398-02866-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/328889 (дата обращения: 24.01.2024). – Режим доступа: для авториз. пользователей.

Краткие теоретические сведения

SOC (Security Operation Center) – центр операций по безопасности. Его цель – непрерывный контроль защищенности и своевременное реагирование на инциденты. Платформа Сбер, как экосистема, представляет сервисы практически во всех сферах жизни, имеет большую территориально распределенную инфраструктуру и сотни тысяч сотрудников. Это требует непрерывного контроля защищенности, своевременного реагирования с учетом совершенствования тактик и техник атак на организации, появления новых вариантов вредоносных программ и мошеннических схем.

Для решения данных задач был построен SOC.

Предпосылки возникновения:

1. Непрерывность и оперативность. Высокая скорость развития цифровой трансформации позволяет быстро выпускать новые приложения и сервисы. Но в то же время порождает киберугрозы. Целью киберпреступников стали данные.

В 2021 г. за дешифровку данных компания Colonial Pipeline заплатила 4,5 миллиона долларов. В результате в ряде штатов США часть АЗС были закрыты ввиду остановок поставок топлива, а цены на бензин резко выросли. Это привело к тому, что авиакомпании American Airlines пришлось отменить рейсы.

2. Проактивность в написании правил детектирования атак. Актуализация средств защиты и их сигнатур является одним из требований безопасности. Данный процесс (настройка обновлений, тестирование) занимает время. В этот период мы остаемся уязвимыми перед атакующим. Злоумышленникам удалось ускориться. Выход эксплойтов занимает считанные часы с момента публикации информации об уязвимости. Это связано с обилием доступного инструментария, постоянно идущих сканирований и наличия специфических поисковых сервисов типа Shodan или PunkSPIDER.

3. Технологичность. При наличии высоких требований к доступности и работоспособности бизнес-процессов компании задачи по своевременному обнаружению и ликвидации инцидента становятся невыполнимы без средств автоматизации.

4. Процессы. Необходимость в них появляется, когда:

- событий, угроз на средствах защиты много;
- требуется формализация взаимодействия между командами.

Нет компаний, которые невозможно взломать. Современные реалии вынуждают писать правила детектирования атак до того, как организация будет атакована.

Выполнение задач по обеспечению защищенности невозможно без современных технологий и процессов.

Работа SOC на примере реального инцидента

Информационное агентство подверглось хакерской атаке с использованием шифровальщика Bad Rabbit. Главный сайт агентства стал недоступен, другие домены компании отображали непонятную информацию.

Сценарий атаки:

1. Злоумышленник взламывает интернет-ресурс и размещает вредоносную нагрузку.

2. Сотрудник компании посещает взломанный ресурс, получая вредоносную нагрузку.

3. Вирус попадает на хост жертвы, заражает АРМ и распространяется по инфраструктуре.

4. Осуществляется шифрование хостов. Может быть реализован другой сценарий. После того, как ВПО заражает хост пользователя, система начинает взаимодействовать со скомпрометированным ресурсом и попадает под контроль злоумышленника. Это позволяет ему проникнуть в структуру компании и продвинуться по сети. SOC – синергия людей, процессов и технологий, обеспечивающая оперативное реагирование на инциденты, проактивное выявление киберугроз, релевантных для организации, и защиту от них. Данное определение через процессы создает связь между людьми, реализующими функции SOC, и техническими средствами, посредством которых они решают задачи предотвращения инцидентов. По локализации функций SOC делится:

1) на внутренний – отдельное подразделение, занимающееся мониторингом реагирования на инциденты и сопровождением технологического стека кибербезопасности. Он интегрирован в про-

цессы организации и ориентирован на ее особенности. Это делает его наиболее эффективным при реагировании на угрозу.

К минусам можно отнести дорогостоящее содержание и время на построение;

2) внешний – компания обслуживается внешним SOC. Его внедрение занимает от нескольких месяцев, компания полагается на специалистов внешнего SOC. Внешний SOC не будет заточен под особенности компании и обнаружение специфичных угроз. Скорость реакции на инциденты также будет страдать из-за необходимости взаимодействия между организациями;

3) гибридный – часть функций делегируется внешнему SOC. Внутренний SOC могут позволить средние и крупные бизнесы. Маленьким компаниям рекомендуется использовать внешнюю или гибридную модель. Сама по себе функция кибербезопасности в отрыве от бизнеса компании не может аргументировать необходимость затрат на найм персонала, закупку средств защиты и продемонстрировать свою нужность компании, а руководство, без демонстрации выгоды, не готово выделять финансирование. Между ними образуется разрыв.

Данную проблему решает переход к управлению кибербезопасностью как к бизнес-функции (ITSM, ITIL). С точки зрения ITSM кибербезопасность совмещается с сервисным подходом, так как ее цель – отсутствие инцидентов, негативно влияющих на защищаемую организацию. ITSM – подход к управлению и организации IT-услуг, направленный на удовлетворение потребностей бизнеса.

Управление IT-услугами реализуется поставщиками данных услуг путем использования оптимального сочетания людей, процессов, технологий.

ITIL – процессы, применяемые в разрезе кибербезопасности:

1. Управление инцидентами. Отвечает за обеспечение оперативного устранения инцидентов.

2. Создание диспетчерской службы Service Desk. По сути является аналогом первых трёх линий SOC.

3. Управление проблемами. Направлен на уменьшение количества инцидентов.

4. Управление конфигурациями. Предназначен для поддержания в актуальном состоянии логической модели инфраструктуры. Отвечает за контроль неизменности настроек конфигурации.

5. Управление изменениями – внесение изменений за счет меньшего влияния на изменяемый процесс системы.

6. Управление уровнем сервиса – выявление и контроль обеспечения установленного уровня сервиса.

В сфере КБ на текущий момент нет общепризнанного стандарта по построению SOC. Однако существуют различные книжки и гайды от различных организаций, так или иначе связанных с КБ, в частности Cisco, MITRE, SANS, NIST и другие. Для реализации принципов ITSM существует сборник документов ITIL. Модель Cyber Kill Chain является подходом к реагированию на инциденты. Данная модель определяет, что необходимо сделать злоумышленнику для проведения успешной атаки. Блокировка хакера на любом из этапов разрывает всю цепочку атаки.

Этапы Cyber Kill Chain:

1. Разведка – выявление особенностей организации, изучение активности компании в соцсетях через рассылки с целью выбора метода атаки.

2. Вооружение – подготовка инструментария для реализации атаки (ВПО, эксплойты, фишинговые страницы).

3. Доставка – отправка вредоносной нагрузки на хост внутри инфраструктуры. После доставки на компьютер происходит запуск вредоносного кода.

4. Эксплуатация уязвимости системы.

5. Установка ВПО. Используется для развития атаки.

6. Контроль над системой – получение удаленного доступа с целью дальнейшего заражения системы.

7. Выполнение действий – хакер отправляет собранные данные или выводит из строя IT-активы.

Kill Chain необходим для моделирования угроз. Этапы цепочки нужно наполнять возможными действиями злоумышленников. Для систематизации информации о методах атак, используемых злоумышленниками, помогает матрица Mitre. Она описывает тех-

ники, используемые злоумышленниками в атаках на корпоративную инфраструктуру.

Для выявления атак существует сценарный подход к реагированию – Use Case.

Он включает:

1. Описание дизайна кибератаки – формулировка угрозы, описание действий злоумышленника, конкретизация, что и как мы детектируем.
2. Правила детектирования. Используются для получения детектора в Ticketing-системе.
3. PlayBook – алгоритм действий по реагированию.

Функции и процессы SOC

Функции SOC:

1. Реагирование на инциденты кибербезопасности:

- мониторинг событий;
- управление инцидентами.

Сопровождает инцидент на протяжении всего жизненного цикла, решает такие задачи, как регистрация, назначение приоритета, необходимость эскалации и хранение информации об инцидентах.

2. Киберразведка (CTI):

- обеспечение ситуационной осведомленности;
- разработка и внедрение Use Case;
- поиск киберугроз и оценка их применимости к организации;
- реагирование на киберугрозы на основе аналитики. Необходима для формирования у руководства понимания о текущем состоянии защищенности, предоставлении прогнозов изменения ландшафта угроз. Информация используется при определении действий по реагированию на киберугрозы.

3. Инжиниринг:

- управление средствами защиты;
- эксплуатация средств защиты;
- поддержка технологического стека SOC. Обусловлена необходимостью постоянно развивать и улучшать технологическую структуру.

4. Управление:

- мотивация и обучение команды SOC;
- организация взаимодействия между командами;
- ведение операционной документации;
- улучшение SOC.

Выполнение описанных функций невозможно без отлаженных процессов.

Процессная модель SOC делится на четыре группы:

1. Реагирование на инциденты:

- управление проблемами, описывает действия для уменьшения возникновения подозрений на инциденты;
- постанализ инцидента отвечает за повышение качества реагирования на инциденты в будущем.

2. Кибербразведка:

- анализ новой информации;
- поиск угроз и их приоритизация.

3. Инжиниринг:

- управление источниками событий кибербезопасности, их мониторинг и валидация;
- управление сбоями SIEM, описываются шаги по максимально быстрому восстановлению данных систем.

4. Управление:

- знанием;
- процедурами;
- операционной документацией;
- рисками;
- процессом постоянного улучшения.

В SOC экосистемы Сбера функционирует 29 процессов, которые описаны в нормативном документе Runbook. Каждый сотрудник может ознакомиться как с процессами, в которых он непосредственно участвует, так и со смежными.

В SOC экосистемы Сбера за реагирование отвечает несколько команд: дежурная смена, отдел реагирования на киберугрозы, сервисный центр информационной безопасности.

Схема реагирования на инциденты. В экосистеме Сбера выделяют шесть уровней приоритета инцидента, который определяется по таблице реализации. На каждый установлен SLA.

Например, для решения инцидента с низким приоритетом отводится 120 часов, а для устранения широкомасштабного инцидента – 2 часа.

Приоритет инцидента зависит от потенциальных последствий: масштаб, финансовый ущерб, влияние на информационные системы, утечка информации, регуляторные риски.

Ущерб от реагирования не должен превысить ущерба от атаки. В связи с этим в экосистеме Сбера используется методика уровня принятия управленческих решений по реагированию на инциденты (Мандат на действия).

Выделяется три команды принятия решений:

- CSIRT – команда реагирования на инциденты;
- EMT – emergency management team;
- орган кризисного управления.

PlayBook – алгоритм действий по реагированию в конкретной ситуации, который включает:

- описание сценария;
- справочную информацию по вносимым изменениям;
- критерии принятия решений;
- описания действий по реагированию.

PlayBook может быть написан как на конкретные правила, так и на общую ситуацию (подозрение на вирусное заражение, комплектацию учетной записи). Для 1-й и 2-й линий действий по PlayBook описание сценария и справочная информация по вносимым изменениям являются обязательными, для 3-й несут рекомендательный характер.

Технологии SOC

Основным элементом SOC является SIEM – система сбора и анализа информации, событий безопасности. Данной системой производится сбор, нормализация и хранение логов, а также корреляция событий по разработанным сценариям, формирование событий с подозрением на инцидент. В SIEM события поступают от различных источников (логи инфраструктуры, средства защиты, DNS).

События позволяют понимать, что происходит в организации, писать правила корреляции, строить аналитические отчеты. На основании правил корреляции SIEM заводит заявку по подозрению на инцидент и отправляет ее в Ticketing-систему.

Ticketing-система – второй по важности элемент. Может быть реализована как на базе SIEM, так и в виде отдельного решения. SOAR позволяет автоматизировать рабочие процессы SOC за счет интеграции со средствами защиты и внутренними системами организации. Выполняет действия для своевременной локализации и уничтожения угроз.

При разборе инцидента аналитик SOC плотно взаимодействует с TIP-системой, которая предназначена для понимания ландшафта угроз на основе контекста информации из внешних и внутренних источников. BI-система – средство для аналитики, визуализации и построения дашбордов. Ее цель – контроль анализа текущей деятельности SOC и оценка эффективности его работы.

Система Behaviour analytics (поведенческая аналитика). Позволяет в режиме реального времени отслеживать аномалии поступающих событий на основе алгоритмов машинного обучения и искусственного интеллекта. Для отклонений существуют системы поведения хостов или пользователей.

Порядок внедрения SOC зависит от уровня его зрелости.

Этап 1. SOC состоит из базовых составляющих – SIEM, Ticketing, системы инжиниринга.

Этап 2. По мере развития SOC обрастает BI и системами IRP (автоматизация реагирования). Системы данного класса расширяют возможности Ticketing, обеспечивая аналитиков SOC средствами автоматизации типовых операций.

Этап 3. Добавляется система TIP. IRP перерастает в SOAR решения, также появляются системы Behaviour analytics.

Далее добавляются системы, выполняющие данные функции с помощью алгоритмов машинного обучения и искусственного интеллекта.

Команда SOC

Команда SOC – единый организм, обеспечивающий защиту организации в киберпространстве.

По функциональной составляющей команду SOC экосистему Сбера можно разделить на 4 направления:

- реагирование на инциденты;
- инжиниринг;
- аналитика киберугроз;
- управление.

За реагирование на инциденты отвечает дежурная смена, состоящая из 1-й, 2-й, 3-й линий. В данное направление входит отдел реагирования, сервисные центры и центр компетенций.

Центр компетенций представлен по направлениям:

– защита периметра сети;
– защита эндпоинтов;
– защита бизнес-приложений;
– защита конфиденциальной информации;
– защита внутренней сети и инфраструктуры.

Сервисные центры распределены территориально с целью оперативного реагирования на инцидент в зависимости от часового пояса.

В группу инжиниринга входит два отдела:

- средств защиты – обеспечивает функционирование сетевых служб;
- средств мониторинга – отвечает за сопровождение систем SOC.

Отдел аналитики киберугроз занимается киберразведкой, анализом появляющихся угроз и их оценкой с точки зрения применимости к экосистеме Сбера, пишет сценарии обнаружения атак. Управление реализуется отделами реагирования и развития. С SOC взаимодействуют отделы:

- Red Team – проводит пентесты систем и контроль функционального состояния SOC;
- Forensic – привлекается в случае подозрения на внутренний фрод, необходимости взаимодействия с МВД.

Контрольные вопросы

1. На какой класс SOC по локализации функций следует ориентироваться компании для развертывания SOC в течение нескольких месяцев?
2. Какие предпосылки возникновения SOC являются ключевыми?
3. Какие технологии обязательно должны присутствовать в SOC базового уровня?
4. Из каких компонентов состоит UseCase?
5. Какую модель рекомендуется использовать при реагировании на инциденты кибербезопасности?

Тесты для самоконтроля

1. Какие элементы включает процесс реагирования на инцидент при наличии SOC?

а) поиск и анализ доступной в Интернете информации об инциденте
б) внеплановая антивирусная проверка устройств
в) информационная рассылка об инциденте на корпоративную почту сотрудников
г) блокировка выделенных каналов с компаниями, которые были атакованы
д) выгрузка образца вредоносного кода для анализа
е) настройка правил в средствах безопасности на основе полученных идентификаторов компрометации
ж) временное ограничение доступа сотрудников в Интернет с рабочих компьютеров
и) проведение внеплановых киберучений

2. Из каких компонентов состоит UseCase?

а) правила детектирования
б) PlayBook
в) описание дизайна кибератаки
г) отчет по расследованию киберинцидента
д) текущая статистика по киберинцидентам
е) политика учетных записей

3. Какие технологии обязательно должны присутствовать в SOC базового уровня? Выберите все правильные ответы.

а) SIEM
б) платформа Threat Intelligence
в) Business intelligence
г) система электронных заявок
д) управление уязвимостями
е) SOAR

Тема 6. УПРАВЛЕНИЕ УГРОЗАМИ И УЯЗВИМОСТЯМИ КИБЕРБЕЗОПАСНОСТИ

Форма проведения занятия – лекция.

Вопросы для обсуждения

1. Какие наиболее прогрессивные техники и алгоритмы в настоящее время реализованы в EDR, SIEM и TI-системах? Каковы тенденции?
2. Как в реальной работе кибербезопасника используется модель нарушителя при оценке угроз и уязвимостей объекта информатизации?
3. Опишите успешные практики по выявлению уязвимостей в ИТ-структуре организации.

Методические указания по проведению занятия

При освоении темы необходимо:

1. Изучить учебный материал по теме 6.
2. Акцентировать внимание на основополагающих понятиях и определениях.
3. Ответить на контрольные вопросы по теме 6.
4. Выполнить тест по теме 6.

Методическое оборудование к занятию: проектор, ноутбук.

Рекомендуемая литература

1. Журавлёва, Н. А. Экономическая безопасность : учеб. пособие / Н. А. Журавлёва ; Петербургский государственный университет путей сообщения Императора Александра I. – Санкт-Петербург : ФГБОУ ВО ПГУПС, 2022. – 78 с. – URL: e.lanbook.com/book/224522 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-7641-1682-2.
2. Краковский, Ю. М. Методы защиты информации : учеб. пособие / Ю. М. Краковский. – Изд. 3-е, перераб. – Санкт-Петербург [и др.] : Лань, 2021. – 234 с. – URL: e.lanbook.com/book/156401 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8114-5632-1.

Краткие теоретические сведения

В современных реалиях ситуационный подход к управлению угрозами может привести к компрометации инфраструктуры организации. Однако если заранее изучить возможные угрозы, можно защитить инфраструктуру и снизить риски.

Термины и определения

Индикатор компрометации (Indicator of compromise, IOC) – объект (IP-адрес, DNS, хеш), наблюдаемый в сети или на конкретном устройстве.

Feed – источник, предоставляющий не только индикаторы компрометации, но и связанный с ними контекст, так как сами по себе индикаторы не имеют смысла.

В качестве контекста могут выступать:

- описание угрозы;
- техники и инструменты злоумышленников;
- принадлежность к какой-либо группировке;
- дополнительные индикаторы.

Тактики, техники и процедуры атакующих (Tactics, Techniques and Procedures, TTP) – описания используемых злоумышленниками методов атаки, основанные на реальных наблюдениях. Позволяют упростить задачу реагирования на инциденты за счет их обобщения в структурированной матрице MITRE ATT&CK и единообразного формата. Детект – факт обнаружения кибератаки.

Уязвимость – недостаток программного/программно-технического средства или информационной системы, который может быть использован для реализации угроз безопасности.

Управление уязвимостями (Vulnerability Management, VM) – процесс выявления, оценки, устранения и составления отчетов об уязвимостях.

Патч-менеджмент (Patch Management) – процесс управления обновлениями ПО.

Threat Intelligence (TI) имеет несколько определений:

1. Знания о мотивах, намерениях и методах злоумышленников, собираемые, анализируемые и распространяемые для помощи специалистам по ИБ и менеджменту по защите критических активов организации на всех уровнях.

2. Основанные на фактических данных знания о существующих или возможных угрозах, которые включают контекст, механизмы, индикаторы, последствия, практические рекомендации и могут быть использованы для принятия решений по реагированию.

3. Набор данных, собранных, оцененных и примененных в отношении угроз, субъектов угроз, эксплойтов, вредоносных программ, уязвимостей и индикаторов компрометации.

Мы считаем первые два определения наиболее подходящими для данного термина, так как в них фигурирует понятие «знание». А оно является результатом нашей работы.

Этапы развития CTI в Сбербанке.

1. Реактивный подход. Реагирование на инцидент происходит после получения информации об угрозе из средств детектирования, мониторинга. Чем позднее мы фиксируем угрозу и реагируем на нее, тем больший ущерб может быть нанесен. Существует вероятность, что к моменту реагирования защитить инфраструктуру не удастся.

2. Детектирование и сокращение времени реагирования до инсталляции основных типов угроз. Детектирование должно происходить на этапе доставки угрозы, а реагирование на нее – в режиме реального времени с учетом автоматизации и механизмов роботизации процессов реагирования.

3. Проактивный подход. Позволяет изучить, задетектировать и среагировать на угрозу до этапа ее доставки.

Изменения возможностей злоумышленника и специалиста по ИБ:

1. Злоумышленник:

- растет квалификация;
- расширяется инструментарий (Red Team Frameworks);
- развиваются возможности автоматизации атак;
- группировки киберпреступников формируются под конкретные отрасли. Все это позволяет злоумышленникам быть на шаг впереди.

2. Специалист по ИБ:

- растет квалификация;
- улучшаются характеристики обмена информацией об угрозах. Остается неизменным время выхода сигнатур, тестирования и установки патчей.

Примеры реализации уязвимостей

Пример 1. Массовое распространение червя WannaCry. Изначально был опубликован эксплойт EternalBlue, позволяющий эксплуатировать одноименную уязвимость. Спустя несколько месяцев появился WannaCry – сетевой червь, который использует EternalBlue для распространения и запуска шифровальщика на скомпрометированных компьютерах. С момента публикации информации об уязвимости, выхода патчей и до появления червя прошло некоторое время, однако никто не успел подготовиться к угрозе. В результате пострадало большое количество организаций во всем мире.

Пример 2. Уязвимость Log4Shell. Так как время на тестирование инфраструктуры было ограничено, попытки эксплуатации угрозы начались, как только появилась информация об уязвимости.

В контексте данных примеров важно отметить, что *работа подразделений CTI начинается с момента публикации информации об уязвимости. Чем быстрее обнаружена и отработана информация об угрозе, тем быстрее можно ее нивелировать и закрыть риски до реализации.*

Управление знаниями

Управление знаниями о киберугрозах делится на категории:

- сбор, систематизация и анализ данных о потенциальных угрозах;
- определение их релевантности и критичности;
- определение необходимых контрмер;
- запуск реагирования;
- выполнение поиска киберугроз в инфраструктуре компании;
- подготовка и распространение аналитических отчетов.

В работу поступают исходные, неструктурированные данные, которые могут быть противоречивыми или нерелевантными. Наша задача – переработать, определить контекст и получить из них информацию. На ее основе появляется понимание, как работает злоумышленник. Это позволяет принимать решения о методах реагирования на атаки.

В Сбербанке используется двухуровневое разделение подходов. Например, на уровне аналитиков есть:

1. Аналитик 1-го уровня:

- изучает неструктурированные данные;
- выделяет индикаторы компрометации и контекст;
- вырабатывает меры митигации;
- направляет контекст аналитику 2-го уровня.

2. Аналитик 2-го уровня:

- проводит поиск угроз по инфраструктуре;
- определяет, была ли реализована угроза ранее;
- решает, что можно сделать, чтобы заблокировать угрозу или поставить на мониторинг;
- вырабатывает правило корреляции в SIEM;
- пишет PlayBook.

Модель представления информации в зависимости от уровня абстракции и количества времени ее использования такова (рис. 8).

Рис. 8. Модель представления информации

Тактическая:

- низкий уровень абстракции;
- долгий период пользования.

Техническая:

- низкий уровень абстракции;
- короткий период пользования.

Стратегическая:

- высокий уровень абстракции;
- долгий период пользования.

Операционная:

- высокий уровень абстракции;
- короткий период пользования.

Тактическая (техники атак) и техническая (индикаторы компрометации) информация используется командами CTI, которые осуществляют реагирование.

Появление нового типа атак – это нечастое событие, в отличие, например, от индикаторов компрометации. Операционно-стратегическая информация используется руководством для принятия конкретных решений.

Одним из аспектов CTI является важность обмена и получения данных об угрозах. Их можно получать из таких источников, как фиды (платные/бесплатные), NIST, ФСТЭК, ФинЦЕРТ. Инструментарий специалиста по CTI:

1. Diamond Model – модель описания злоумышленника.
2. Cyber Kill Chain – модель описания этапов атаки.
3. MITRE ATT&CK – модель описания этапов и техники атак.
4. CVSS – система установления критичности и приоритизации уязвимостей.
5. Форматы обмена данными об угрозах:

- язык обмена данными (STIX) позволяет написать любую угрозу и структурировать ее по определенным полям;
- описание вредоносных программ (YARA) является аналогом файловой сигнатуры;
- стандарты описания сигнатуры сетевых атак (Suricata);
- описание поведенческих шаблонов (Sigma) позволяет загрузить поведенческие шаблоны в SIEM систему с целью задетектировать вредоносную активность в инфраструктуре.

Анализируя угрозу, важно ответить на пять ключевых вопросов:

1. Является ли уровень угрозы критическим, высоким, средним или низким?
2. Предрасположена ли инфраструктура компании к атаке?

3. Каким способом распространяется атака?
4. Какие TTP используют злоумышленники?
5. Было ли зафиксировано влияние?

Пирамида боли Дэвида Бьянки описывает уровни сложности индикаторов компрометации, которые злоумышленники используют при атаках. Пирамида позволяет описать подход, который эффективно использовать для детектирования. Чем выше уровень, тем сложнее злоумышленнику обойти метод детектирования.

Рассмотрим ее уровни, где через тире указывается метод детектирования:

1. Тривиальный – Хеш-сумма.
2. Легкий – IP-адрес.
3. Незначительно сложный – Доменное имя.
4. Довольно трудный – Сетевое взаимодействие/артефакты на хосте.
5. Сложный – Инструменты.
6. Очень сложный – Тактика, техники и процедура.

Данные методы детектирования можно разделить на три группы:

1. IOC-based:

- хеш-сумма;
- IP-адрес;
- доменное имя;
- сетевое взаимодействие/артефакты на хосте.

2. Tool-based: инструменты.

3. TTP-based: тактика, техники и процедура. Самым главным в CTI является получение знаний о конкретной угрозе, так как оно позволяет предпринять меры по блокировке угрозы и снижению рисков. Управление уязвимостями.

Существует как минимум три типа уязвимостей:

1. Архитектурные ошибки.
2. Ошибки конфигурации.
3. Ошибки в программном обеспечении.

Наибольшую сложность вызывает решение архитектурных ошибок. Например, существует методика спуфинга, при которой мошенник выдает себя за надежный источник, чтобы получить доступ к данным или информации. Такая подмена может происходить через веб-сайты, IP-адреса (ARP протокол), серверы.

Для устранения уязвимостей могут применяться меры:

- компенсирующие (установка патча);
- системные (накрутка политики, блокировка угрозы).

Модель CVSS для приоритизации уязвимости. При определении приоритетов мы основываемся на том, что у каждой уязвимости есть скоринг (базовый и временной), контекст, определяющий, как данная уязвимость влияет на конкретную инфраструктуру. Данные метрики можно рассчитать с помощью специальных калькуляторов, которые рассчитывают степень риска и критичности уязвимости. Чем она критичнее, тем больший приоритет ей будет присвоен.

Пример расчета CVSS 3.1

Анализируя уязвимость, важно ответить на шесть ключевых вопросов:

1. Насколько уязвимость критична?
2. Уязвимость в продукте или компоненте?
3. Есть ли в инфраструктуре продукт/компонент с уязвимостью?
4. Есть ли эксплойт?
5. Опубликованы ли способы митигации?
6. Детектится ли попытка эксплуатации?

Процесс управления уязвимостями является цикличным и состоит:

- из мониторинга уязвимостей и угроз, оценки применимости;
- оценки уязвимостей;
- определения методов и приоритетов устранения;
- устранения уязвимостей (мы предлагаем меру и контролируем ее применение в инфраструктуре);
- контроля устранения.

Процесс управления уязвимостями в экосистеме Сбера

Действия при обнаружении уязвимости:

1. Ищем информацию о том, насколько она критична/не критична.

2. Поиск информации о способах ее устранения/митигации.

3. Принимаем решение о релевантности на основе различных баз данных (Service manager, UCMDB, Inventory). Мы должны хоро-

шо знать инфраструктуру, поэтому все базы должны быть актуальными и непротиворечивыми.

4. Если уязвимость релевантна, принимаем решение о проведении сканирования в инфраструктуре, привлечении RedTeam.

5. Переоценка уязвимости. Необходимо проанализировать, в какой части инфраструктуры мы нашли уязвимость, насколько она является критичной с точки зрения нахождения в инфраструктуре, является ли это уязвимостью на периметре или уязвимость находится в изолированном сегменте.

6. Устранение.

7. Контроль устранения.

8. Отчетность. Отдельной частью процесса управления уязвимостями, требующей внимания, является актуализация данных об активах и их классификация критичности.

Ландшафт киберугроз и примеры

Ландшафт киберугроз связан со спецификой финансовой организации. Мы воспринимаем угрозу в соответствии с тем, на кого она направлена (инфраструктуру банка или клиентов). Например, фишинг – не только рассылки вредоносных программ, но и регистрация вредоносных сайтов, куда собираются персональные данные клиентов (номера карт, учетные данные). С ландшафтом угроз связано применение MITRE ATT&CK, которая используется в качестве методологии построения правил детектирования. Можно выделить следующие проблемы применения данной методологии:

- часть техник описана абстрактно, нет общего детекта;
- невозможно детектить все техники;
- зависимость способов детектирования от конкретной реализации инфраструктуры. Требуется адаптация правил детекта под конкретную организацию. Необходимо рассматривать каждую угрозу по отдельности.

Примеры угроз.

1. Ботнет. На первом этапе пытается заразить как можно большее количество устройств и взять их под свое управление. На втором – провести атаку (например, DDoS). Когда мы видим DDoS-атаку, мы снимаем все IP-адреса в моменте и с помощью сканера

Shodan собираем информацию по конкретному адресу. По ботнетам мы можем определить, какой сервис на нем открыт. В нашем примере это веб-камера (обладает характерным портом 554 RTSP).

2. Вредоносное ПО. Существуют сложности при детектировании вредоносных программ, поэтому уже на логах EDR систем мы собираем информацию об активности определённых процессов. В данном случае рассмотрим одну из вредоносных программ по ее графу, какую цепочку процессов она порождает. Так, например, этапы 7, 8, 9 встречались в одной из первых версий программы. Обнаружив, что данные этапы позволяют быстро задетектировать программу, злоумышленники перестроили цепочку. При анализе вредоносной программы необходимо не только определить, как она работает, какой риск несет, но и построить цепочку с целью провести детектирование на основе логов. По действиям также можно определить, используются ли противодействия обнаружению или обход средств защиты. Например, обход User Account Control легко обнаружить с помощью активности в части реестра.

3. Уязвимости и сетевые атаки на примере Log4j. Проблема заключается в том, что в логах не всегда видно выделенную выше строку. Ее можно обфусцировать и обойти средства детектирования. Вредоносное ПО (APT, MINER) может быть использовано с эксплойтом.

4. Группировки. Diamond Model – модель описания группировок злоумышленников состоит из следующих сущностей:

- злоумышленник;
- инфраструктура, используемая злоумышленником;
- возможности (характеризуются качеством и количеством);
- жертва.

Для установления группировки важно определить ее цели, страну (для правительственных группировок), технические возможности (ВПО, эксплойты, скомпрометированные сертификаты). Так, одна из группировок направила письмо от лица компании «Ростех» с целью распространения вредоносной программы. В программе использовался домен динамического DNS сервиса, что характерно для определенного типа группировок. Анализ вредоносной про-

граммы посредством OSINT инструмента Maltego позволил определить IP-адрес и местоположение, откуда производилась атака.

Инструменты злоумышленников:

- Cobalt Strike – позволяет автоматизировать действия в инфраструктуре жертвы;
- Impacket внутри сети – позволяет скомпрометировать инфраструктуру Active Directory. Процессы и люди CTI Процессы CTI.

Автоматизация процессов CTI Группы процессов в экосистеме Сбера разделены на следующие категории:

- инжиниринг;
- реагирование на инциденты;
- CTI;
- управление.

Процессы CTI:

- управление данными;
- анализ информации;
- реагирование на основе аналитики КБ;
- разработка и настройка сценариев;
- приоритизация угроз;
- запрос аналитической информации;
- управление уязвимостями;
- поиск угроз.

Автоматизация процессов CTI происходит посредством Threat Intelligence Platform (рис. 9). Платформа не учитывает информацию об инфраструктуре. Если она разрабатывается не в организации, внесение изменений затруднительно и затратно. В связи с этим Сбербанк создал свою платформу SberTIP.

В ней реализованы два модуля: Threat Intelligence Platform и Vulnerability Management.

Обрабатываемую информацию мы кладем в инфраструктуру в виде кейсов. Под кейсом мы понимаем аналитический отчет, описание. С помощью модуля графовой аналитики мы изучаем структуру связей между объектами и приземляем их на граф.

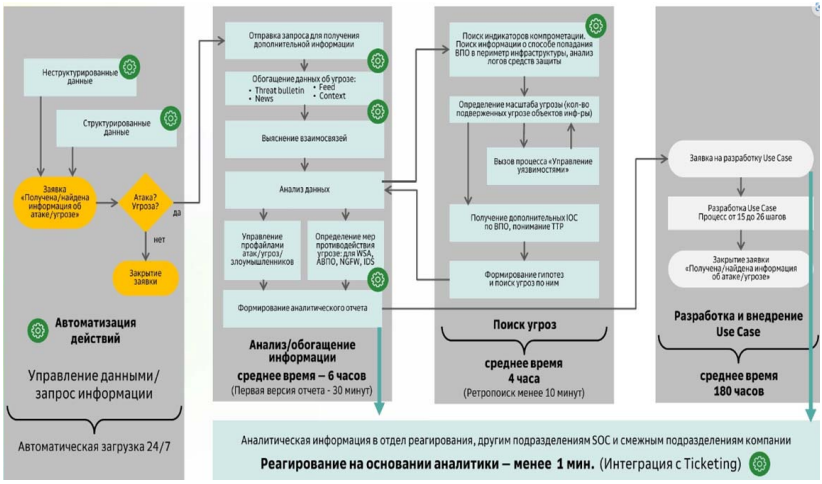


Рис. 9. Автоматизация процессов CTI в Сбербанке (https://vk.com/wall-149273431_1678?ysclid=lsixkupcro313057603)

Команда CTI

По функциональной составляющей подразделение CTI можно разделить на четыре направления:

- анализ информации;
- управление уязвимостями;
- поиск киберугроз в инфраструктуре;
- разработка и настройка сценариев.

Контрольные вопросы

1. Какая модель применяется для описания хакерских группировок?
2. Какие существуют категории информации CTI?
3. Что входит в функционал подразделений кибербезопасности?
4. Какие существуют стадии кибератаки в рамках модели Kill Chain?
5. Что понимается под управлением уязвимостями?

Тесты для самоконтроля

1. Что понимается под управлением уязвимостями?

а) управление обновлениями программного обеспечения

б) выявление, оценка, устранение уязвимостей безопасности в информационных системах и составление отчетов

в) выявление, оценка, устранение уязвимостей безопасности в программном коде на всех этапах разработки

г) исследование и оценка методов эксплуатации уязвимостей хакерскими группами

2. Какая из перечисленных моделей применяется для описания хакерских группировок?

а) Kill Chain

б) MITRE ATT&CK

в) Diamond Model

г) OWASP Top 10

3. К какой категории информации CTI следует отнести сведения о техниках атаки?

а) технической

б) тактической

в) операционной

г) стратегической

4. Что не входит в функционал подразделений кибербезопасности?

а) обнаружение уязвимостей

б) оценка критичности

в) устранение уязвимостей

г) подготовка отчетности по киберугрозам

5. Что относится к используемым в CTI индикаторам компрометации? Выберите все правильные ответы.

а) IP-адрес

б) описание угрозы

в) инструменты злоумышленников

г) хеш

д) DNS

6. На каких стадиях кибератаки в рамках модели Kill Chain возможно проактивное реагирование? Выберите все правильные ответы.

а) разведка
б) вооружение
в) доставка
г) инсталляция
д) управление
е) действие

Тема 7. ПРАКТИКИ БЕЗОПАСНОЙ РАЗРАБОТКИ И DEVSECOPS

Форма проведения занятия – лекция.

Вопросы для обсуждения

1. Каким образом должна отличаться разработка и сопровождение информационных систем, в которых происходит обмен конфиденциальной информацией, от разработки и сопровождения информационных систем, где вся информация считается общедоступной?
2. Как правильно организовать обмен данными между разными видами информационных систем?
3. Как наиболее рационально в учебной деятельности применить практики безопасной разработки и DevSecOps?

Методические указания по проведению занятия

При освоении темы необходимо:

1. Изучить учебный материал по теме 7.
2. Акцентировать внимание на основополагающих понятиях и определениях.
3. Выполнить практическую работу 1 и 2.
4. Ответить на контрольные вопросы по теме 7.
5. Выполнить тест по теме 7.

Методическое оборудование к занятию: проектор, ноутбук.

Рекомендуемая литература

1. Кийко, П. В. Цифровые технологии : учеб. пособие / П. В. Кийко ; Омский государственный аграрный университет имени П.А. Столыпина. – Омск : ФГБОУ ВО Омский ГАУ, 2023. – 108 с. – URL: e.lanbook.com/book/349799 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-907687-34-9.
2. Краковский, Ю. М. Методы защиты информации : учеб. пособие / Ю. М. Краковский. – Изд. 3-е, перераб. – Санкт-Петербург [и др.] : Лань, 2021. – 234 с. – URL: e.lanbook.com/book/156401 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8114-5632-1.

Краткие теоретические сведения

Безопасность приложений (Application Security) – раздел кибербезопасности, в котором объектом защиты является программное обеспечение и его потенциальные уязвимости.

Причем основное внимание уделяется предотвращению появления уязвимостей, а не их обнаружению в уже готовом продукте. Application Security затрагивает практически каждый артефакт и шаг производства программного обеспечения.

Что защищаем:

- данные;
- алгоритмы;
- файлы;
- деньги;
- иные активы.

Через эксплуатацию уязвимости можно:

- парализовать или осложнить деятельность компании;
- модифицировать или украсть информацию, использовать ее для шантажа или нанесения репутационного ущерба;
- похитить денежные средства.

Граница между такими понятиями, как фича и баг, достаточно размыта и зависит от того, под каким углом зрения мы на них смотрим. Баг при правильном использовании может стать фичей. И наоборот, даже задокументированная особенность приложения может быть проэксплуатирована злоумышленниками как уязвимость. Самые популярные уязвимости описаны в методологии OWASP TOP 10.

Чем отличаются Application Security, SSDLC и DevSecOps?

Application Security включает меры по повышению защищенности приложения путем обнаружения, исправления и предотвращения уязвимостей, которые появляются в результате ошибок на этапе проектирования или написания программного кода.

SSDLC (Secure Software Development LifeCycle) – жизненный цикл безопасной разработки программного обеспечения, который включает жизненный цикл разработки SDLC (Software Development LifeCycle).

Пионером в создании подходов SDLC и SSDLC выступила компания Microsoft.

Процесс SSDLC строится по классической каскадной модели:

Этап 1. Формирование потребности: формирование основных требований по ИБ.

Этап 2. Проектирование:

- формирование перечня рисков;
- разработка модели угроз;
- формирование требований с учетом рисков и модели угроз;
- включение требований в техническое задание;
- отражение требований в рамках технического проекта.

Этап 3. Разработка и тестирование:

- анализ уязвимостей архитектуры;
- статический и динамический анализ приложения;
- fuzzing.

Этап 4. Ввод в эксплуатацию:

- анализ уязвимостей ПО;
- тестирование на проникновение.

Этап 5. Сопровождение:

- тестирование ПО на наличие уязвимостей;
- мониторинг уязвимостей в используемых библиотеках;
- устранение уязвимостей.

Этап 6. Вывод из эксплуатации/внесение изменений: контроль вывода из эксплуатации/начало цикла.

Таким образом, на каждом из этапов разработки SSDLC предполагает ряд мер, которые относятся к обеспечению безопасности. SSDLC является частью Application Security.

DevSecOps – это безопасный конвейер, который является частью SSDLC для конвейера DevOps, в который добавлены технологии информационной безопасности. Причем они присутствуют на всех этапах – от проектирования до выпуска продукта.

Практики и инструменты Application Security

Шаг 1. Проектируем безопасно. Прежде чем перейти к разработке, решение надо спроектировать. В проектировании один из важнейших компонентов – архитектура. Хорошая архитектура по-

зволяет не только обеспечить функциональность и безопасность продукта, но и дает возможность его развивать и масштабировать, сохранять и совершенствовать его безопасность.

Рекомендуем стандарт ASVS 4.0 от OWASP в качестве источника, в котором описаны многие лучшие практики, применявшиеся при создании безопасной архитектуры. Для того чтобы гарантировать соответствие разрабатываемого продукта требованиям безопасности, необходимо учитывать ГОСТы и ISO стандарты.

Шаг 2. Пишем код безопасно. Следующий этап в создании продукта – разработка. С точки зрения Application Security задача ставится как написание безопасного кода.

Здесь есть несколько ключевых моментов:

- самые опасные места в программе возникают там, где одна функциональность взаимодействует с другой (приложение – СУБД, приложение – ОС, интеграционные взаимодействия);
- рекомендуется использовать безопасные конструкции, предоставляемые фреймворками, языками, конструкторами шаблонов;
- важно применять лучшие практики программирования, следить за чистотой кода, потому что безопасный код – это прежде всего качественный код;
- для проверки потенциально опасных фрагментов кода советуем использовать плагины, которые встраиваются в среду разработки и позволяют тестировать код еще на этапе программирования.

Шаг 3. Тестируем приложение. После разработки тестируем следующие объекты:

- исходный код;
- дистрибутивы;
- конфигурационные файлы;
- запущенные приложения в динамике. Практики тестирования бывают ручные и автоматизированные.

Среди ручных практик выделим Code Review и Penetration Testing. Code Review – это просмотр кода с точки зрения его критичных участков, не очень хорошего стиля программирования и использования тех или иных методов. При наличии компетенции данная практика весьма эффективна.

Penetration Testing – значительно более сложная и дорогостоящая практика. Данное тестирование проводится периодически в качестве аудита на безопасность. Она хорошо дополняет другие практики и позволяет находить такие дефекты, которые не находятся автоматизированными средствами.

Автоматизированные практики тестирования приложений включают:

1. Статический анализ кода (SAST: Static Application Security Testing). Это самая популярная и простая в имплементации практика. Она позволяет находить не очень хорошие языковые конструкции, захардкоженные пароли, осуществлять автоматизацию Code Review.

У SAST есть ряд недостатков:

- высокий уровень ложных срабатываний;
- патчи к статистическим анализаторам отстают от новых версий фреймворков примерно на полгода-год.

2. Анализ OpenSource компонент (OSS/SCA). Использование готовых компонент, которые можно скачать из Интернета. Это очень упрощает и убыстряет разработку, но в то же время несет достаточно высокие риски. Потому что есть общедоступные базы с эксплойтами именно для этих компонент.

Основной и самый полный перечень уязвимостей в компонентах расположен здесь: https://nvd.nist.gov/.

Небезопасные OpenSource библиотеки встречаются не только в собственном коде, но и в системном ПО. Поэтому важно периодически обновлять системный софт.

3. Bytecode анализ (BCA: Bytecode and Container Analysis) – более редкая практика, при которой анализируется уже собранный дистрибутив. Позволяет выявлять секреты и конфиденциальные данные даже с учетом обфускации кода. Используется преимущественно для мобильных приложений.

4. Динамический анализ приложения (DAST: Dynamic Application Security Testing). Суть этой практики в том, что, запуская приложение, мы реализуем различные стандартные проверки на типовые уязвимости. Это очень тяжеловесная и дорогостоящая

практика, требующая наличия тестового стенда, но в итоге точность тестирования получается высокой.

5. Тестирование бизнес-функционала (BAST: Behavioral Application Security Testing). Такое тестирование, как правило, проводят на приемке продукта эксперты кибербезопасности. Поэтому данная практика позволяет проверить требования кибербезопасности к функционалу ПО и составить список замечаний в бизнес-терминах.

6. Интерактивный анализ приложений (IAST: Interactive Application Security Testing). Встраиваемое решение, которое может идентифицировать место исправления в коде.

Основным недостатком является сложность реализации, поскольку непросто найти подходящий инструмент для такого тестирования.

Шаг 4. Выпускаем приложение. Итак, тестирование завершено. В результате найдено некоторое количество уязвимостей. Какие-то изъяны в коде удается исправить, но ряд уязвимостей останется. На этом шаге важно оценить риски, которые будут учитывать возможные последствия от эксплуатации уязвимости, а также предложить подходящие меры митигации.

Например:

- установить патч/обновить ПО или библиотеку;
- убедиться, что уязвимый функционал OpenSource библиотек не используется;
- применить внешние средства защиты;
- обеспечить online-реагирование на попытку эксплуатации и моментальное отключение узла сети или приложения;
- убедиться, что уязвимость не эксплуатируется в вашем окружении.

Шаг 5. После выпуска приложения применяется практика Application Security – Bug Bounty. Она предусматривает выплату награды этичным хакерам за обнаружение проблем в безопасности сервисов и приложений компании. Это дает производителям программного обеспечения способ найти уязвимости, которые не удалось выявить в процессе разработки.

Практические рекомендации для применения Application Security в бизнесе

При выборе практик Application Security и подходов к их применению следует учитывать многие факторы:

- размер компании;
- направление бизнеса;
- зрелость процессов разработки и кибербезопасности в компании;
- тип разрабатываемых приложений, используемый технологический стек;
- вид обрабатываемой информации и функционал приложений;
- количество разрабатываемого ПО.

Реализация практик Application Security в компаниях в зависимости от их размера выглядит следующим образом.

StartUp. На этапе стартапа достаточно учитывать принципы безопасного проектирования и разработки.

Middle. Для средних компаний (с точки зрения бизнеса, количества клиентов или ПО, которое они разрабатывают) можно использовать Code Review и простейшие статические анализаторы. Они не требуют больших трудозатрат и времени на сопровождение.

High. Для крупных компаний (с точки зрения зрелости процессов) необходимо добавить более сложные практики тестирования.

Например, пентест, динамический анализ, Bytecode анализ. Для самых зрелых компаний можно добавить практику **Bug Bounty**. Как решать проблему ложных срабатываний? Прежде всего надо понять – это действительно ложное срабатывание или просто неэксплуатируемые уязвимости, которые подсвечивает инструмент. Полезно также анализировать статистику по истинно положительным срабатываниям. Если есть комплексные проблемы, то истинные срабатывания позволят обнаружить систематические ошибки.

Подходы к процессам Application Security:

1. Децентрализованный. Есть несколько команд, каждая из которых разрабатывает приложение или часть приложения. Команды заботятся о реализации мер безопасности, не согласовывая это друг с другом.

Например, команда 1 использует Code Review и SAST, команда 2 – только Code Review, команда 3 – SAST и OSS. Это не очень зрелый подход с точки зрения безопасности.

2. Централизованный. Характерен для ситуации, когда команды вообще не заботятся о безопасности. Продукт разработки сканирует на безопасность внешний подрядчик или внутренние эксперты по безопасности и присылают список обнаруженных дефектов обратно в команды (возможно, сами что-то исправляют). Один из недостатков такого подхода в том, что он не несет ценности в развитии культуры кибербезопасности.

3. Оптимальный. В этом подходе реализованы лучшие элементы двух предыдущих. А именно: команды разработки заботятся о безопасности продукта. И есть еще центр компетенций за пределами команд, который рассказывает, обучает, помогает внедрять наиболее эффективные практики безопасности. Это самый правильный подход с точки зрения развития киберкультуры.

Пример реализации SSDLC в экосистеме Сбера

В DevOps конвейере запущено несколько инструментов безопасности: статика, Open Source, динамический анализ. Для централизованной работы инструментов безопасности создается собственная платформа Application Security. Она позволит не только тестировать разные решения, но и смотреть корреляцию между результатами, статистику, формировать аналитику и создавать собственный продукт. В DevOps конвейере реализованы механизмы контроля Quality Gate.

Также используется стоп-лист для приложений, в которых необходимо устранить уязвимости как можно скорее. Для того чтобы отслеживать эти процессы, мы пользуемся дашбордами, которые сами проектируем и разрабатываем.

Немного статистики. Каждый день в конвейере экосистемы Сбера запускается более 7000 сканов. Над этим работает больше 1,5 тысячи команд. Для сопровождения решений есть несколько линий поддержки. Кроме того, в самом конвейере присутствуют линии первой поддержки, которые помогают с вопросами по эксплуатации, инструментам разработки и статического анализа.

Культура Application Security

Культура определяется мышлением, отношением людей к тому, что мы делаем, определяется идеей. Application Security разделяет принцип «сдвига влево» в производстве. Это означает, что чем раньше удается выявить потенциальные проблемы и уязвимые места, тем дешевле их исправить.

Поэтому компетенции ИБ и понимание угроз безопасности должны присутствовать у всех участников процесса производства приложения, но в разном объеме и разных ракурсах.

Для формирования культуры ИБ используется Security Awareness, то есть практика развития осведомленности в вопросах безопасности.

С этой целью Сбербанк делает следующее:

- пишутся статьи;
- проводятся лекции, практические семинары;
- создаются обучающие курсы;
- делятся опытом;
- используются средства информирования – каналы, рассылки, новостные ленты;
- развиваются ИТ-сообщества в университетах и компаниях;
- организовываются CTF-соревнования;
- проводятся лабораторные исследования.

Эти средства служат достижению следующих целей:

- повышение осведомленности о возможных последствиях кибератак;
- обсуждение примеров эксплуатации уязвимостей;
- формирование другого видения безопасности как неотъемлемого атрибута качественного продукта, его конкурентного преимущества.

В командах разработки ключевую роль в этом контексте играют Security Champions – сотрудники, которые являются точкой входа в команду разработки и евангелистами безопасности.

Их роль – способствовать формированию в команде культуры применения лучших практик Application Security. Поэтому знания Security Champions не могут быть чисто теоретическими.

Эти специалисты умеют:

- практически применять знания Application Security в разработке приложений, работать над созданием приложения в любой роли;
- определять риски ИБ и меры их митигации;
- формировать культуру ИБ и внедрение лучших практик Application Security в команде.

Контрольные вопросы

1. В каких случаях наиболее вероятно появление уязвимостей?
2. Какая часть методологии Secure Software Development Lifecycle (SSDLC) находится за рамками подхода DevSecOps?
3. Что является достоинством автоматизированного статического анализа кода (SAST)?
4. В одном из бизнес-приложений вашей организации найдена уязвимость. Какие планы митигации вы предложите?
5. На что направлен основной фокус внимания Application Security?

Тесты для самоконтроля

1. В каких случаях наиболее вероятно появление уязвимостей?

а) при наличии пользовательского интерфейса

б) при несоблюдении принципов ООП

в) при вызове функции с переменным числом аргументов

г) на стыке взаимодействия приложения и операционной системы и/или приложения и базы данных

2. Какая часть методологии Secure Software Development Lifecycle (SSDLC) находится за рамками подхода DevSecOps?

а) разработка требований к безопасности приложения

б) разработка исходного кода

в) создание инсталляционного пакета

г) развертывание в инфраструктуре

3. Что является недостатком автоматизированного статического анализа кода (SAST)?

а) высокая стоимость

б) высокий уровень ложно-положительных срабатываний для сложных проверок

в) не подходит для анализа мобильных приложений
г) низкая производительность

4. В одном из бизнес-приложений вашей организации найдена уязвимость. Какие планы митигации из предложенных допустимы?
а) установить исправленную версию приложения
б) убедиться, что найденная уязвимость не может быть проэксплуатирована в вашем окружении
в) исключить файлы приложения из числа сканируемых антивирусом
г) ограничить функционал приложения, чтобы исключить эксплуатацию уязвимости
д) оценить степень риска и согласовать с руководством организации его принятие
е) установить последние обновления операционной системы на компьютерах

5. На что направлен основной фокус внимания Application Security?
а) обнаружение уязвимостей в готовом продукте
б) предотвращение появления уязвимостей
в) исправление уязвимостей в готовом продукте
г) классификация уязвимостей в приложениях

6. Какие утверждения, касающиеся Secure Software Development Lifecycle (SSDLC), являются верными?
а) SSDLC включает SDLC
б) SSDLC включает Application Security
в) процесс SSDLC включает шаги: формирование требований, проектирование, разработка и тестирование, ввод в эксплуатацию, сопровождение, внесение изменений или вывод из эксплуатации (в случае завершения цикла)
г) пионером в создании подхода SSDLC выступила компания Apple

Тема 8. УПРАВЛЕНИЕ РИСКАМИ КИБЕРБЕЗОПАСНОСТИ

Форма проведения занятия – лекция.

Вопросы для обсуждения

1. Какой подход по управлению кибербезопасностью наиболее эффективный?
2. Каким образом управление рисками должно быть отражено в документах, касающихся политики информационной безопасности организации?
3. Виды метрик для определения приемлемости рисков.

Методические указания по проведению занятия

При освоении темы необходимо:

1. Изучить учебный материал по теме 8.
2. Акцентировать внимание на основополагающих понятиях и определениях.
3. Выполнить практическую работу 4.
4. Ответить на контрольные вопросы по теме 8.
5. Выполнить тест по теме 8.

Методическое оборудование к занятию: проектор, ноутбук.

Рекомендуемая литература

1. Кийко, П. В. Цифровые технологии : учеб. пособие / П. В. Кийко ; Омский государственный аграрный университет имени П.А. Столыпина. – Омск : ФГБОУ ВО Омский ГАУ, 2023. – 108 с. – URL: e.lanbook.com/book/349799 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-907687-34-9.
2. Краковский, Ю. М. Методы защиты информации : учеб. пособие / Ю. М. Краковский. – Изд. 3-е, перераб. – Санкт-Петербург [и др.] : Лань, 2021. – 234 с. – URL: e.lanbook.com/book/156401 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8114-5632-1.

Краткие теоретические сведения

Согласно Положению ЦБ РФ № 716-П от 08.04.2020, риск кибербезопасности (КБ) – это риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения информационной безопасности, прикладного ПО автоматизированных систем и приложений, несоответствием указанных процессов деятельности организации.

На рис. 10 представлены группы рисков кибербезопасности, включающие кредитные, операционные, рыночные риски, риски ликвидности и прочие риски.

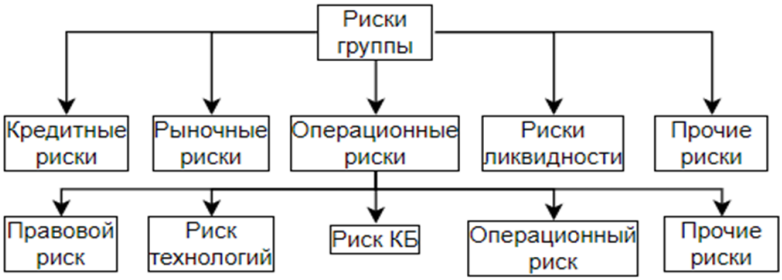


Рис. 10. Группы рисков кибербезопасности

Цель управления рисками КБ – обеспечение баланса между развитием бизнеса и достаточным уровнем КБ (рис. 11), формирование эффективной системы управления, которая учитывает регуляторный и риск-ориентированный подходы.

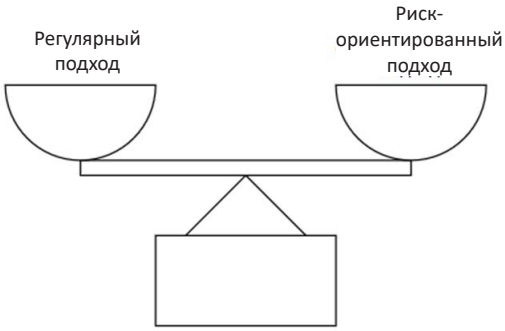


Рис. 11. Подходы к построению эффективной системы управления рисками

Регуляторный подход предусматривает выполнение внешних и внутренних нормативно-правовых требований.

Риск-ориентированный – направлен на определение допустимого и принимаемого уровня риска, который позволит вводить в эксплуатацию и реализовывать продукты банка без максимальной проработки вопросов безопасности.

Ключевые задачи по управлению рисками:

- соблюдение баланса между затратами на защиту и получаемым эффектом;
- определение приемлемого диапазона уровня риска;
- своевременное информирование руководства о новых идентифицированных рисках, их уровне;
- развитие риск-культуры – общепринятых в организации правил поведения и ценностей в вопросах управления рисками, которые соблюдаются и которым привержены топ-менеджмент и сотрудники.

Система управления риском кибербезопасности

Система управления рисками КБ в банках представлена в виде пирамиды. На верхнем уровне – Внутренние нормативные документы (ВНД) и Правила функционирования системы, на среднем – Люди и Процессы, которые выполняют эти Правила, на нижнем – Технологии. Нормативные документы:

- законодательство РФ и нормативно-правовые акты ЦБ РФ;
- ГОСТы, международные требования и стандарты ISO, требования Базельского комитета по банковскому надзору и Европейского банковского управления (EBA);
- ВНД компании: политики, стандарты, методики. Положение ЦБ РФ № 716-П от 08.04.2020 способствовало развитию системы управления рисками КБ банков. В нем впервые зафиксировано понятие киберриска в составе операционного. Оно обязывает управлять рисками ИБ в составе общей системы управления рисками, а также регламентирует постоянное взаимодействие между службами КБ и управления рисками. В Положении закреплено участие правления компании в решении вопросов по рискам КБ, необходимость привлекать внутренний аудит для регулярных проверок.

Присутствует отдельный раздел с требованиями по ведению базы и оценке потерь от событий риска КБ (инцидентов).

Дополнительно в положении зафиксировано 13 контрольных показателей, которые отражают картину в разрезе мошенничества у клиентов.

Один из важных процессов управления рисками КБ – построение 3-х линий киберзащиты:

1. Бизнес-подразделения предварительно идентифицируют риски в бизнес-процессах, принимают меры по защите на своем уровне.

2. Специальные подразделения отвечают за методологию, контроль, независимую оценку, выставление лимитов. В банках это подразделение центрального подчинения «Риски», блок «Риски» и департамент кибербезопасности.

3. Внутренний аудит проверяет эффективность работы системы, выполнение внутренних и внешних требований. В случае несоответствия передает информацию руководству и контролирует устранение несоответствия.

Такая организация процесса позволяет банкам минимизировать конфликт интересов между принятием рисков, ограничением и контролем их уровня, а также аудитом системы управления риском.

Дополнительно в роли 4-й линии выступает регулятор – ЦБ и внешние аудиторские организации.

Ключевые области по управлению рисками КБ:

- риски в ИТ-инфраструктуре;
- риски в разработке;
- риски в бизнес-процессах;
- риски мошенничества.

Для каждого направления применяются инструменты риск-ориентированного подхода: сканеры уязвимости, ATI-платформы, статический анализ кода, антифрод-система.

Управление рисками в инфраструктуре

Платформа осуществляет ежедневный мониторинг различных источников на предмет выявления новых уязвимостей. В случае их выявления анализируется применимость каждой уязвимости к инфраструктуре. Если она применима, риск оценивается с учетом риск-факторов влияния и вероятности.

Далее определяется перечень автоматизированных систем, которые подвержены этой уязвимости. Соответствующим командам поддержки из ИТ-подразделений ставятся задачи с перечнем мероприятий и сроками устранения.

В качестве инструментов контроля применяется повторное сканирование на уязвимости, чтобы убедиться, что коллеги выполнили задачу по ее устранению.

Риск-ориентированный подход помогает приоритизировать задачи для подразделений ИТ, чтобы в первую очередь устранить наиболее уязвимые места в системе. Зависимость уровня риска от уровня влияния и вероятности определяется через произведение значений влияния и вероятности.

Влияние определяется по факторам критичности для системы, применимости к инфраструктуре, рейтинга CVSS.

Вероятность определяется по факторам затронутого сегмента сети, наличия эксплойта, CTI-тренда. Факторам присваиваются баллы. По формуле производятся вычисления. В результате получается значение от 0 до 1, которое соотносится со шкалой для технологических рисков. Дальнейшая работа ведется исходя из получившегося уровня риска.

Управление рисками в процессах

Например, у бизнес-подразделения возникла потребность в изменении процесса разработки продукта. Оно обращается в управление экспертизы КБ.

Управление выставляет требования КБ для изменения процесса с последующим контролем. Если бизнес-подразделение не может выполнить требования, возникает вопрос: каковы последствия их невыполнения или выполнения в другой срок? Ответ на данный вопрос – это формулировка будущего риска КБ. По нему оформляется заявка на оценку, которая вносится в автоматизированную систему. По каждому риску назначается ответственный специалист, который организует оценку, привлекая профильных экспертов из подразделений банков. Команда экспертов проводит консолидированную оценку риска и готовит отчет. В нем указывается уровень риска и меры митигации.

План митигации – набор технических мероприятий со сроками и ответственными. Отчет направляется бизнес-заказчику.

Ему дается несколько дней на принятие решения. После оценки риск аллоцируется на данное подразделение. Оно будет нести ответственность в случае реализации риска.

Аллоцирование рисков связано с системой лимитов: подразделение не сможет принять на себя риски выше определенного уровня и количества. Ему будет необходимо реализовывать планы митигации по уже аллоцированным рискам, чтобы принять новый. На основании отчета бизнес-подразделение принимает решение и направляет в департамент КБ служебную записку, в которой фиксирует план митигации со сроками и принятие уровня риска. Пока план митигации не реализован, информация об ответственности подразделения передается в отчеты руководству. После выполнения плана риск переоценивается. Если он снизился, то перестает учитываться в системе лимитов и включаться в отчеты руководству. Согласно риск-ориентированному подходу риски снижаются до приемлемого уровня, а не снимаются полностью, поскольку это влечет увеличение затрат.

Применяемые технологии

В Сбербанке внедрена GRC-система, которая автоматизирует процесс оценки рисков, подготовки отчетов, разработки планов митигации и контроля их выполнения.

Примеры GRC-систем: Security Vesion, R-Vesion, ePlat4m.

Функционал GRC-системы в Сбербанке:

- формирование сотрудником заявки на оценку риска КБ;
- заполнение опросных листов экспертами;
- расчет рейтинга и уровня риска;
- ведение реестра рисков;
- мониторинг обработки рисков, составление планов митигации;
- экспресс-оценка – онлайн-калькулятор, позволяющий бизнес-подразделению самостоятельно методом перебора критериев и факторов оценить предварительный уровень риска.

Управление рисками в соответствии с ISO 27005.

По международному стандарту ISO 27005 процесс управления рисками КБ включает несколько этапов.

1. Идентификация рисков:

1.1. Выявление отклонений от требований КБ и регистрация выявленного риска командой управления экспертизы КБ.

1.2. Инициативное информирование о возможных рисках и самооценка сотрудниками банков.

1.3. Анализ угроз и уязвимостей на платформе кибербезопасности.

1.4. Ведение базы событий риска КБ-инцидентов.

Карта рисков – классификатор, который позволяет систематизировать учет рисков компании. Чтобы ее построить, необходимо изучить все инциденты, которые ранее происходили в компании и отрасли в целом, отчеты аудита. По итогам получаются группы рисков, присущих компании (рис. 12). Далее группы детализируются.

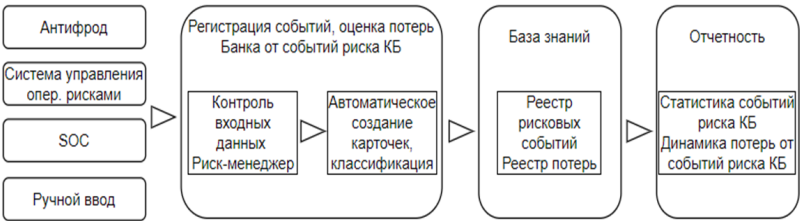


Рис. 12. Классификация событий согласно требованиям 716-П

Например, для банков группы рисков:

- утечка конфиденциальной информации;
- внешнее/внутреннее мошенничество;
- недоступность активов;
- нарушение целостности активов;
- нарушение процессов управления КБ.

2. Оценка уровня рисков = вероятность реализации риска × ценность актива.

2.1. Методика ISO 27.

2.2. Методика банков. Учитывается большой набор риск-факторов для определения ценности актива и вероятности реализации риска. Вероятность вычисляется по набору комбинаций: выявляет-

ся угроза, для нее определяется группа нарушителей, которые могут ее реализовать. Определяется подмножество уязвимостей, которые могут использовать нарушители при реализации данной угрозы.

Определяется подмножество мер защиты, которые могут противостоять нарушителю при реализации угрозы с использованием уязвимости. По каждому набору комбинаций определяется вероятность, затем вычисляется общая вероятность.

По итогам оценки получается нормированное значение от 0 до 1, которое сопоставляется с качественной шкалой уровней (рис. 13):

- низкий: 0–0,25;
- средний: 0,25–0,5;
- высокий: 0,5–0,75;
- критический: 0,75–1.

Уровень риска: R = V(влияние) × P(вероятность)

Риск	Рейтинг	Диапазон очков
AA	Критичный	≥ 0.85
A	Высокий	≥ 0.6
B	Средний	≥ 0.3
C	Малый	≥ 0

Рис. 13. Качественная шкала уровней

2.3. Самооценка: стандартный инструмент для управления операционными рисками, но в КБ употребляется редко. Во всех подразделениях банков есть риск-координаторы, которые отвечают за бизнес-процессы подразделения и оценивают возможные риски, в том числе риски КБ. Они также оценивают эффективность мер защиты и прогнозируют возможные финансовые потери. О выявленных рисках координаторы сообщают в департамент КБ. В самооценке принимают участие сотрудники банков.

Таким образом, команда департамента КБ получает информацию о рисках и о их количественной оценке непосредственно от

подразделения, которое отвечает за процесс и чаще всего является единственным обладателем данной информации. Самооценка может проводиться как ежегодно, так и в динамическом режиме, чтобы оперативно корректировать суммы капитала, заложенные под потери от рисков.

3. Обработка риска:

3.1. Избегание – отказ от процесса/продукта/уязвимой системы.

3.2. Передача – страхование (например, рисков утечки информации, потерь от мошенничества); аутсорсинг (передача сервиса сторонней организации).

3.3. Снижение – реализация плана митигации, чтобы уровень риска опустился до приемлемого уровня.

3.4. Принятие. Решения по рискам КБ должны принимать лица с соответствующим уровнем полномочий. Для этого существует матрица принятия решений по рискам (рис. 14). Решения по рискам низкого уровня могут принимать владельцы процесса или продукта. Решения по высоким рискам находятся в полномочиях топ-менеджмента.

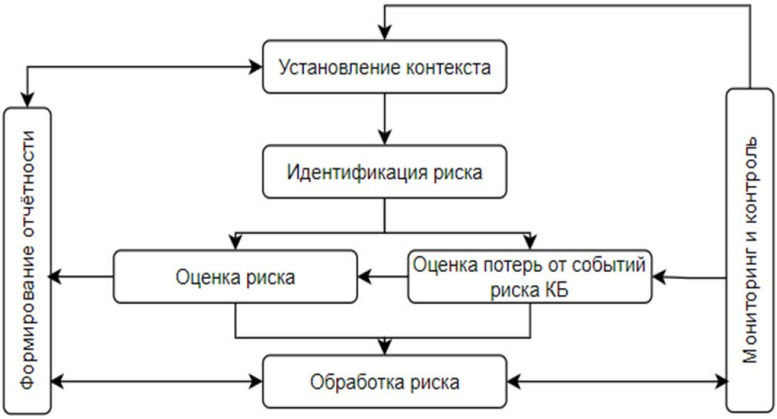


Рис. 14. Матрица принятия решений по рискам

Для принятия решений по стратегическим рискам и рискам, затрагивающим деятельность нескольких подразделений, целесообразно иметь в организации коллегиальный орган – комитет по управлению риском КБ. В него включаются представители под-

разделений КБ и ИТ, бизнес-подразделений. Комитет позволяет дополнительно вовлекать топ-менеджмент в вопросы управления КБ, что стратегически важно.

Для эффективного выстраивания процесса управления рисками в банке принята единая процедура принятия рисков. Когда запускается новая инициатива или продукт и руководителю надо принять решение об их реализации, проводится оценка по направлениям нефинансовых рисков.

Риски КБ тесно связаны с другими операционными рисками. Каждый риск оценивается в денежном эквиваленте и заносится в единую таблицу. Руководитель должен принимать решения, обладая полной информацией о всех возможных рисках. Единая процедура принятия рисков позволяет вести консолидированный учет взаимосвязанных рисков.

4. Мониторинг и контроль рисков КБ в банках осуществляется в рамках отслеживания реализации мер защиты плана митигации.

Отдел аудита управления экспертизы КБ проверяет выполнение требований КБ. Он занимается не только пересмотром сроков реализации мер и переоценкой рисков, но и ведением отчетности о рисках КБ, которая поступает руководству.

Сбербанк ведет мониторинг и контроль рисков КБ в GRC-системе, но для этого достаточно и таблицы в Excel. Это единый консолидированный перечень всех рисков с датами, на которые риски принимаются, и датами плана митигации.

Риски не могут приниматься бессрочно. В таблице можно фильтровать по датам, которые подходят к завершению, запрашивать статус, проверять реализацию мер. Такими простым способом можно реализовать мониторинг.

Подготовка отчетности по рискам КБ осуществляется по нескольким уровням:

- базовый: отчет по каждой оценке риска с указанием уровня, планом митигации, сценарием реализации;
- средний: консолидированная отчетность для крупных подразделений банков в формате дэшборда, на котором можно посмотреть превышение метрик и конкретные риски;

• высокий: контрольные и сигнальные значения показателей, утвержденных Положением ЦБ РФ № 716-П, для топ-менеджмента. Отчеты готовятся ежемесячно и ежеквартально.

Один из вариантов отчетов – утверждение рисков в формате метрик к аппетиту рисков, т. е. максимальному уровню риска, который компания готова на себя принять. Лимиты аппетита к риску выражают в денежном эквиваленте.

Например, объем от риска, который компания готова понести за год по всем направлениям риска. В банках – собственная система лимитов, которая включает 20 метрик – показателей по проблемным направлениям. Система схематически представлена в виде тепловой карты в разрезе подразделений. Зеленый – нет превышения, желтый – есть превышения и план митигации, красный – нарушен срок или отсутствует план. Большая часть рисков КБ связана с инфраструктурой.

5. Оценка потерь. Помогает учитывать тренды, идентифицировать новые риски, строить связь потенциальных рисков, влиять на переоценку по рискам, по которым случились потери. Происходит сбор событий риска (инцидентов) из нескольких систем. Данные передаются в систему по рискам. По рискам, где есть потери, проводится оценка.

Виды потерь:

• прямые – отражаются в бухгалтерском учете;
• непрямые – косвенные (упущенная выгода), качественные (невозможно оценить в денежном эквиваленте), потенциальные (еще не реализовались).

При оценке потерь анализируются все события по операционному риску, чтобы не упустить события КБ в текстовом поле без соответствующей пометки. Для этого применяется модель AI, которая анализирует поля и классифицирует их. Методика оценки косвенных потерь: косвенные потери = финансовые потери + репутационные.

Финансовые потери включают:

• расходы на реагирование, устранение последствий и расследование причин (привлечение внешнего аудитора, восстановление работоспособности, замена выведенного из строя оборудования, переработки сотрудников, их командирование);

• расходы на коммуникацию и взаимодействие с лицами, затронутыми событием (привлечение внешнего колл-центра, уведомления, SMS-сообщения);

• экономические последствия (недополученные доходы от простоя систем, потери работоспособности, утечки информации);

• предотвращение возможных потерь и подобных событий в будущем (перевыпуск банковских карт, стоимость повышения лояльности клиентов через маркетинговые инструменты, план мероприятий для снижения вероятности потерь).

Репутационные потери вычисляются посредством умножения числа клиентов, которые охвачены негативной публикацией в СМИ и соцмедиа, на CLTV (средний ожидаемый доход на клиента) и на чувствительность аудитории к публикации.

Данная методика оценки косвенных потерь является собственной разработкой Сбербанка. Качественная оценка потерь проводится по градуированным шкалам. Исходя из типа информации определяется качественный уровень потерь в зависимости от критичности для системы или бизнес-процессов и длительности простоя.

6. Риск-культура – принятые в организации нормы и правила по управлению рисками, риск-ориентированное мышление руководства и понимание сути риска сотрудниками. Развивать риск-культуру необходимо в том числе для проведения самооценки и инициативного информирования о рисках КБ.

Главный инструмент – обучение сотрудников.

Ключевые международные документы по управлению рисками

- ISO/IEC 27005:2018 «Information technology – Security techniques – Information security risk management»;
- ISO/IEC 31010:2019 «Risk management – Risk assessment techniques»;
- NIST SP 800-39 «Managing Information Security Risk»;
- NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations».

Приемлемый уровень риска определяется в соответствии с целями компании. В Сбербанке не допускается утечка конфиденциальной информации, поэтому стоит лимит на принятие высоких рисков утечки. Но можно принять высокие риски мошенничества. По остальным направлениям также устанавливаются лимиты.

Определение приемлемого уровня рисков – лимитирование и метрики аппетита к риску.

План мероприятий для снижения рисков прорабатывается исходя из конкретной ситуации и зависит от требований КБ, которые необходимо выполнить. Он часто включает компенсирующие мероприятия для снижения рисков.

Схема качественной оценки рисков:

1. Поступает запрос от бизнес-подразделения, назначается риск-менеджер.

2. Риск-менеджер анализирует предметную область, заполняет поля в системе, описывает область оценки.

3. Риск-менеджер рассчитывает ценность актива по факторам: сумма фактических значений факторов делится на сумму максимальных значений. Получается коэффициент от 0 до 1.

4. Формируются опросные листы: выбираются применимые угрозы для реализации риска. Определяется группа нарушителей и уязвимости, которые нарушители могут использовать при реализации угрозы, меры защиты. Опросный лист может корректироваться в дальнейшем по просьбам профильных оценивающих экспертов.

5. Привлекается экспертная группа из 3–4 человек, которая оценивает по вероятностной шкале каждую комбинацию угроз, групп нарушителей, уязвимостей и мер защиты. Шкала включает значения: «Точно нет», «Низкая», «Средняя», «Высокая», «Очень высокая», «Точно да».

6. Автоматически рассчитывается вероятность: каждому значению шкалы соответствует числовой коэффициент. Система производит вычисления, эксперты выставляют только качественные значения.

7. Производится итоговый расчет уровня риска: вероятность реализации угрозы умножается на ценность актива. Получается нормированное число от 0 до 1, которое соотносится с качественной шкалой.

Таким образом вычисляется качественный уровень риска.

Контрольные вопросы

1. Какие существуют риски кибербезопасности?
2. В каком нормативном документе была произведена формализация единых требований к системе управления риском информационной безопасности для финансовых организаций?
3. Организация приняла решение отказаться от использования WhatsApp и Telegram на корпоративных устройствах. Каким будет вариант обработки риска утечки конфиденциальной информации корпоративных данных этой организацией?
4. К какой линии защиты относятся функции по разработке методологии управления риском кибербезопасности и независимой оценки уровня риска?
5. Для чего в организации необходимо устанавливать аппетит к риску КБ?

Тесты для самоконтроля

1. К какой группе рисков относятся риски кибербезопасности?

а) рыночные
б) ликвидности
в) операционные
г) кредитные

2. В каком нормативном документе была произведена формализация единых требований к системе управления риском информационной безопасности для финансовых организаций?

а) ФЗ №395-1
б) Положение ЦБ №716-П
в) Указание ЦБ №3624-У
г) ФЗ №161

3. Организация приняла решение отказаться от использования WhatsApp и Telegram на корпоративных устройствах. Каким будет вариант обработки риска утечки конфиденциальной информации корпоративных данных этой организацией?

а) избегание

б) передача

в) снижение

г) принятие

4. К какой линии защиты относятся функции по разработке методологии управления риском кибербезопасности и независимой оценки уровня риска?

а) первая линия

б) вторая линия

в) третья линия

г) ко всем вышеперечисленным

5. Для чего в организации необходимо устанавливать аппетит к риску КБ? Выберите все правильные ответы.

а) определить максимальный уровень риска, который организация готова принять для достижения своих целей

б) определить, каким рискам подвержена компания

в) определить, какие потери неприемлемы для организации

г) осуществлять сбор данных по инцидентам

Тема 9. ПРОБЛЕМАТИКА ПРИМЕНЕНИЯ СКЗИ В ЭДО

Форма проведения занятия – лекция.

Вопросы для обсуждения

1. Почему в реальных системах используется такое разнообразие алгоритмов криптографической защиты информации и для каких ситуаций подходят те или иные алгоритмы?
2. Какой алгоритм, на ваш взгляд, является самым криптостойким?
3. Современные криптографические протоколы, их уязвимости, вопросы импортозамещения.

Методические указания по проведению занятия

При освоении темы необходимо:

1. Изучить учебный материал по теме 9.
2. Акцентировать внимание на основополагающих понятиях и определениях.
3. Выполнить практическую работу 3.
4. Ответить на контрольные вопросы по теме 9.
5. Выполнить тест по теме 9.

Методическое оборудование к занятию: проектор, ноутбук.

Рекомендуемая литература

1. Кийко, П. В. Цифровые технологии : учеб. пособие / П. В. Кийко ; Омский государственный аграрный университет имени П.А. Столыпина. – Омск : ФГБОУ ВО Омский ГАУ, 2023. – 108 с. – URL: e.lanbook.com/book/349799 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-907687-34-9.
2. Краковский, Ю. М. Методы защиты информации : учеб. пособие / Ю. М. Краковский. – Изд. 3-е, перераб. – Санкт-Петербург [и др.] : Лань, 2021. – 234 с. – URL: e.lanbook.com/book/156401 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8114-5632-1.
3. Надёжность и защита информации автоматизированных систем : учеб. пособие / М. Н. Краснянский, В. Г. Матвейкин, А. В. Затонский [и др.] ; Тамбовский государственный техниче-

ский университет. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2022. – 95 с. – URL: e.lanbook.com/book/355145 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8265-2460-2.

Краткие теоретические сведения

В рамках этой темы нами будет рассмотрена проблематика применения СКЗИ в таких прикладных вещах, как система электронного документооборота (ЭДО). Мы обсудим, с какими вызовами сталкиваются организации при внедрении ЭДО. На примере Сбербанка посмотрим, как можно решать основные проблемы при переходе на ЭДО.

Рис. 15. Преимущества ЭДО

ЭДО: две стороны медали

В любом процессе всегда имеется две стороны. ЭДО – не исключение.

1. Рассмотрим лицевую сторону медали (рис. 15, слева):

• Мобильность предполагает, что с любого мобильного телефона, в любой точке мира сейчас можно подписать документ и отправить.

• Гарантированность доставки. Текущие средства информационных систем и средства информационной системы электронного документооборота позволяют, в отличие от Почты России, гаран-

тировать доставку документа до адресата, контрагента либо участника сделки.

• Прозрачность процесса.

В отличие от бумажного документооборота участник может отследить, где сейчас находится подписанный им документ.

Каждый этап жизненного цикла документа квитируется системой ЭДО и подписывается электронной подписью. То есть документ сформировали, подписали, отправили. Факт отправки также подтверждается электронной подписью. Документ поступил в личный кабинет контрагента, этот факт тоже подписывается. Все артефакты собираются, хранятся в системе ЭДО. В случае конфликтных ситуаций они могут быть представлены в суд, т. е. прозрачность – 100 %.

• Скорость. В отличие от всех бумажных видов электронный составляется за секунды.

2. Обратная сторона медали (рис. 15, справа). Рассмотренные преимущества ЭДО подразумевают:

- разветвленную архитектуру;
- высокие требования к каналам передачи данных;
- возможность утечек;
- вероятность DDoS-атак на информационные системы (в частности, весной 2022 г.);
- необходимость поддержания обратного формата совместимости документов (это означает, что через 15–20 лет будет возможность прочитать документы, сгенерированные в электронном виде, проверить электронную подпись);
- жесткие временные рамки: в отличие от бумажного документооборота подписать документ в ЭДО «задним числом» невозможно.

Как указанные проблемы решаются в Сбербанке?

В банке есть SOC, который позволяет отслеживать DDoS-атаки и прочие вещи, связанные с утечками. Существует также фонд проектной документации – своего рода архив, в котором «складируются» дистрибутивы программного обеспечения. С целью резервирования каналов связи банк заключает договоры с крупнейшими операторами связи, магистральными провайдерами. Каждое решение проходит через архсовет. Электронный документооборот по-

зволяет обеспечивать конфиденциальность передаваемых данных за счет соответствующих средств защиты.

В основном применяются СКЗИ. Их надо поддерживать в актуальном состоянии: следить за сертификатами, обновлять, внедрять парольные ролевые политики, которые позволяют предотвращать доступ к личным кабинетам. В Сбербанке это решается за счет СКЗИ канального и программного уровня.

Внедряются виртуальные рабочие станции, системы удаленного доступа и ролевой модели, DLP-системы, IRM-системы защиты документов. Крайне важно физическое разделение зон (EMZ, DMZ, Дельта, Сигма, Альфа). Самая защищенная зона, не имеющая прямого выхода в Интернет, – Пенал. Там располагаются критически важные системы, в том числе системы удостоверяющего центра. Современная система ЭДО не может существовать без комплексного подхода, развитой IT-инфраструктуры.

Набор политик, стандартов, регламентов позволяет правильно распределить зоны ответственности и порядок действий в случае конфликтных ситуаций. Согласно последним исследованиям, затраты на электронный и бумажный документооборот сопоставимы.

Для крупных компаний, в том числе для Сбербанка, на первый план выходит не экономия, а удобство использования.

ЭДО – это удобный поиск и удобное архивирование. Основное назначение СКЗИ в системах ЭДО – это обеспечение юридической значимости.

В соответствии с Федеральным законом № 63-ФЗ существует три вида электронной подписи:

- простая;
- усиленная квалифицированная (УКЭП), используется без дополнительных соглашений;
- усиленная неквалифицированная (УНЭП), используется с соглашением.

В банке есть СберДокс – внутренняя система ЭДО. Там применяется как УНЭП, так и УКЭП.

3. При отправке документов через систему межведомственного электронного взаимодействия в госорганы, при приеме сотрудников на работу используется УНЭП, а также соответствующее

соглашение. СфераКурьер – бизнес-продукт банка. Клиенты – юридические лица – могут обмениваться юридически значимыми электронными документами. Также СКЗИ используется для идентификации пользователей и обеспечения конфиденциальности.

В совокупности это обеспечивает высокий уровень кибербезопасности. Сбербанк использует сертификаты усиленной электронной подписи, сертифицированные СКЗИ и криптографическую аутентификацию по протоколу HMAC для облачных сервисов электронной подписи. ЭДО возможен только с применением СКЗИ.

Что будет, если СКЗИ не применять?

Обеспечение юридической значимости. Целостность документа достигается средствами системы, а неотказуемость от авторства достигается логами системы. Здесь фактически доверие происходит в отношении самой системы ЭДО без дополнительных средств.

Согласно Федеральному закону № 63-ФЗ, криптография при использовании простой электронной подписи не нужна. Целостность документа средствами системы теоретически и технически можно обеспечить, но это требует повышенного внимания – так же, как и логи системы.

Соответственно, и простая электронная подпись (логин, пароль, биометрия, палец, лицо) плюс соглашение тоже очень пограничная вещь. Но для нерисковых операций применяется простая электронная подпись плюс соглашения.

Например, в СБОЛе, когда вы нажимаете «Подтвердить перевод», используется простая электронная подпись. И в кадровом ЭДО есть варианты использования простой электронной подписи. Каждый сотрудник при приеме на работу/при кадровых изменениях подписывает соответствующее соглашение.

Для идентификации пользователей может быть применен цифровой ID либо биометрия, но конфиденциальность передаваемых данных без СКЗИ может достигаться только штатными мерами или самими средствами системы. Для идентификации пользователей в Сбербанке используются Сбер ID и SmartBIO. При этом конфиденциальность передаваемых данных обеспечивается не штатными мерами, а сертифицированными СКЗИ. Применение средств

криптографической защиты информации в ЭДО позволяет обеспечивать высокий уровень кибербезопасности.

Проблемы при использовании средств с СКЗИ

Прежде всего встраивание CSP. Необходимо проводить оценку влияния окружения. Однако в режиме DevOps это делать невозможно. Выход есть – реализация концепции «непрерывной сертификации» и согласование подхода с регулятором. Еще одна проблема – встраивание SDK. Любой SDK, существующий на рынке, содержит ограниченный набор клиентских сценариев и пользовательского интерфейса.

Здесь поможет кастомизация решений с привлечением вендоров и регулятора.

4. Сбербанк участвует в профильных комитетах (ТК-26, ТК-362), ведет прямой диалог с регуляторами и вендорами, как и некоторые другие крупные компании (*Мегафон, ВТБ, Тинькофф*). Однако большинство игроков рынка занимают выжидательную позицию.

Из регуляторных проблем самой острой является отсутствие на рынке сертифицированных средств УЦ и ЭП, которые можно использовать для предоставления облачного сервиса КЭП. После регистрации приказа ФСБ аккредитованные УЦ смогут оказывать сервис облачной КЭП при условии прохождения дополнительной аккредитации и наличии сертифицированных СКЗИ.

Решение простое – сертификация новых средств и аккредитация удостоверяющих центров. Также проблемы связаны с ограниченным перечнем дистанционных способов идентификации при выдаче сертификатов УКЭП.

Есть четыре способа дистанционной идентификации:

- УКЭП на УКЭП, когда по квалифицированным действующим сертификатам можно пройти дистанционную идентификацию;
- загранпаспорт с биометрией;
- использование единой системы идентификации и единой биометрической системы;
- ПЭП ЕСИА как дополнительный способ идентификации для выдачи неквалифицированных сертификатов. Решить проблемы можно расширением способов дистанционной идентификации (УНЭП на УНЭП, использование ПЭП ИС).

Организационные проблемы. Полная реализация требований документации на СКЗИ тяжело осуществима и затратна. В этой связи необходима работа с вендором и регулятором по гармонизации требований для соблюдения баланса между «удобно» и «безопасно».

Сбербанк, как и другие крупные игроки, для решения этих вопросов совершенствует внутренние процедуры, регламенты, проактивно работает с регулятором и вендорами.

Вызовы и перспективы

За последние 1,5–2 года мы видим колоссальное снижение количества аккредитованных УЦ. По состоянию на 2-й квартал 2021 года их было более 50, в 3-м квартале 2022 года – 42. Предполагается, что это должно привести к снижению мошенничества в сфере электронной подписи, а также повышению доверия к институту электронной подписи.

Однако проблемы остаются прежними: у каждого аккредитованного УЦ есть свои доверенные лица, которые должны проводить идентификацию (будущего владельца, квалифицированного или неквалифицированного сертификата). К ним доверия пока нет.

Кроме того, никаких других проверок (кроме документарных) при первичной аккредитации нет. Для получения «звания» аккредитованного УЦ достаточно просто собрать пакет документов и отправить в Минцифры. При этом никто не приезжает на место, не смотрит, как организован доступ к серверам УЦ, какие средства там установлены.

5. Со стороны государства возникают предпосылки национализации сферы электронной подписи. С 2020 года вступил в силу Федеральный закон от 27.12.2019 № 476-ФЗ, установивший, что три государственных УЦ могут выдавать электронные подписи по подведомственности:

- ФНС – для юридических лиц, индивидуальных предпринимателей;
- Казначейство – для федеральных органов исполнительной власти;
- ЦБ – для финансово-кредитных организаций.

Существуют также предпосылки национализации сферы платформ подписания. Все это может привести к контролю хозяйственной деятельности субъектов ЭДО. Но в этом есть и минусы для бизнеса – перестройка всех клиентских сценариев. Если раньше Сбербанк как аккредитованный УЦ мог выдавать клиентам квалифицированный сертификат, то сейчас выдает его через УЦ федеральных Госуслуг.

Сбербанк стал доверенным лицом УЦ ФНС. При этом все равно существует зависимость от сторонних поставщиков сертификатов, то есть банк обращается в УЦ ФНС.

Возникает вопрос, кто платит за недоступность сервисов. Из-за этой тенденции наблюдается миграция на аналоги электронной подписи.

Бизнес старается выйти из-под действия Федерального закона № 63-ФЗ и использовать, например, не электронную подпись, а электронную квитанцию/электронный документ.

Развитие облачных платформ очень важно как крупному бизнесу, так и клиенту. К концу 2023 года появились первые аккредитованные УЦ, которые предоставляют сервис дистанционной квалифицированной электронной подписи. Проблема – в отсутствии легитимного облачного сервиса УКЭП.

Бизнес вынужден переходить на мобильную подпись. Там есть определенные ограничения, связанные с хранением ключей на устройстве. Это легитимно, но не всегда хороший клиентский путь. УНЭП и простая электронная подпись в критически значимых сделках и бизнес-процессах должны исчезнуть, останется только УКЭП.

В отношении дистанционных сервисов существует усиленная электронная подпись Госуслуг.

Преимущества:

- можно получить за 5 минут (главное – иметь подтвержденную учетную запись);
- доступность гос. сервисов;
- все документы – в одной корзине.

Последнее преимущество одновременно является и проблемой: когда все документы в одном месте, то в случае утечки база данных будет полностью утеряна.

Все граждане РФ имеют возможность взаимодействия в электронном виде с органами исполнительной власти, муниципальными учреждениями.

Проблемы – те же (все документы в одной корзине, зависимость от стороннего поставщика услуг и самое главное – кто заплатит за ущерб). Внедрение МЧД – автоматизация проверки полномочий подписантов.

Среди проблем – дополнительные расходы бизнеса на внедрение, неочевидная выгода, отсутствие порядка реализации.

Появляются новые способы дистанционной идентификации при выдаче сертификатов ЭП (УНЭП на УНЭП и ПЭП ИС УЦ). Это удобно для клиента, а для бизнеса происходит сокращение затрат.

6. Законодательная база ЭДО как предмет не преподается, научной литературы по этой теме нет.

Однако существует ряд законов и подзаконных актов, на которых держится текущая инфраструктура ЭДО РФ.

1. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 02.07.2021) «Об электронной подписи» (с изм. и доп., вступ. в силу с 04.08.2023).

2. Постановление Правительства РФ от 15.07.2021 № 1207 «О проведении эксперимента по использованию усиленной электронной подписи при предоставлении услуг и осуществлении иных действий с использованием федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

3. Постановление Правительства «О внесении изменений в отдельные акты Правительства Российской Федерации» № 1786 от 07.10.2022.

4. Постановление Правительства РФ от 01.12.2021 № 2152 «Об утверждении Правил создания и использования сертификата ключа проверки усиленной неквалифицированной электронной подписи в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для

предоставления государственных и муниципальных услуг в электронной форме».

5. Распоряжение Правительства РФ от 10.04.2021 № 933-р (ред. от 24.09.2021) «Об утверждении состава Правительственной комиссии, уполномоченной на принятие решения об аккредитации удостоверяющих центров».

6. Постановление Правительства РФ от 28.11.2011 № 976 (ред. от 25.09.2018) «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

7. Постановление Правительства РФ от 28.12.2020 № 2309 «Об утверждении требований к порядку предоставления владельцам квалифицированных сертификатов сведений о выданных им квалифицированных сертификатах с использованием единого портала государственных и муниципальных услуг».

8. Постановление Правительства РФ от 29.06.2021 № 1044 (ред. от 04.02.2022) «Об утверждении Положения о федеральном государственном контроле (надзоре) в сфере электронной подписи».

9. Приказ Минкомсвязи России от 13.04.2012 № 108 (ред. от 11.04.2017) «Об обеспечении осуществления Министерством связи и массовых коммуникаций Российской Федерации функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров» (вместе с «Положением об информационной системе головного удостоверяющего центра, функции которого осуществляет федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи») (зарегистрировано в Минюсте России 26.04.2012 № 23950).

10. Приказ Минцифры России от 29.10.2020 № 559 «Об утверждении Административного регламента предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по аккредитации удостоверяющих центров и Административного регламента осуществления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственного контроля (надзора) за соблюдением аккредитованными 7 удостоверяющими центрами требований, которые установлены Федеральным законом «Об электронной подписи» и на соответствие которым эти

удостоверяющие центры были аккредитованы» (зарегистрировано в Минюсте России 03.11.2020 № 60735).

11. Приказ Минцифры России от 13.11.2020 № 584 «Об утверждении Требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей» (зарегистрировано в Минюсте России 02.12.2020 № 61213).

12. Приказ Минцифры России от 02.11.2021 № 1134 «Об утверждении Порядка передачи реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи, в случае прекращения деятельности аккредитованного удостоверяющего центра» (зарегистрировано в Минюсте России 30.11.2021 № 66141).

13. Приказ Минцифры России от 08.12.2021 № 1313 «Об утверждении индикативных показателей, применяемых при осуществлении федерального государственного контроля (надзора) в сфере электронной подписи».

14. Приказ Минцифры России от 07.12.2021 № 1312 «Об утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) в сфере электронной подписи» (зарегистрировано в Минюсте России 18.02.2022 № 67348).

15. Приказ Минцифры России от 08.11.2021 № 1138 «Об утверждении Порядка формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, включая требования к формату предоставления такой информации» (зарегистрировано в Минюсте России 30.11.2021 № 66117).

16. Приказ Минцифры России от 19.11.2020 № 603 «Об утверждении требований к порядку действий аккредитованного удостоверяющего центра при возникновении обоснованных сомнений относительно лица, давшего поручение на использование хранимых ключей электронной подписи, а также при приостановлении (прекращении) технической возможности использования хранимых

ключей электронной подписи, включая информирование владельцев квалифицированных сертификатов ключей проверки электронной подписи о событиях, вызвавших приостановление (прекращение) технической возможности использования хранимых ключей электронной подписи, об их причинах и последствиях» (зарегистрировано в Минюсте России 22.12.2020 № 61708).

17. Приказ Минцифры России от 26.11.2020 № 624 «Об утверждении перечня угроз безопасности, актуальных при идентификации заявителя – физического лица в аккредитованном удостоверяющем центре, выдаче квалифицированного сертификата без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой информационной системы персональных данных, обеспечивающей обработку, сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, а также хранении и использовании ключа электронной подписи в аккредитованном удостоверяющем центре» (зарегистрировано в Минюсте России 22.12.2020 № 61689).

18. Приказ ФСБ России от 04.12.2020 № 554 (ред. от 13.04.2021) «Об утверждении Порядка уничтожения ключей электронной подписи, хранимых аккредитованным удостоверяющим центром по поручению владельцев квалифицированных 8 сертификатов электронной подписи» (зарегистрировано в Минюсте России 30.12.2020 № 61971).

19. Приказ ФСБ России от 20.04.2021 № 154 «Об утверждении Правил подтверждения владения ключом электронной подписи» (зарегистрировано в Минюсте России 31.05.2021 № 63700).

20. Приказ ФСБ России от 27.12.2011 № 795 (ред. от 29.01.2021) «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» (зарегистрировано в Минюсте России 27.01.2012 № 23041).

21. Приказ ФСБ России от 27.12.2011 № 796 (ред. от 13.04.2022) «Об утверждении Требований к средствам электронной подписи

и Требований к средствам удостоверяющего центра» (зарегистрировано в Минюсте России 09.02.2012 № 23191).

22. Постановление Правительства РФ от 21.02.2022 № 222 «Об утверждении Правил представления заинтересованным лицам документа о полномочиях физического лица в случае, предусмотренном частью 2 статьи 17.1 Федерального закона «Об электронной подписи».

23. Постановление Правительства РФ от 21.02.2022 № 223 «Об утверждении организационно-технических требований к порядку хранения, использования и отмены указанных в статьях 17.2 и 17.3 Федерального закона «Об электронной подписи» доверенностей».

24. Постановление Правительства РФ от 21.02.2022 № 224 «Об утверждении требований к нормативным правовым актам федеральных органов исполнительной власти, устанавливающим порядок представления доверенности в предусмотренном пунктом 2 части 1 статьи 17.2 Федерального закона «Об электронной подписи» случае, и требований к порядку представления доверенности в предусмотренном пунктом 2 статьи 17.3 Федерального закона «Об электронной подписи» случае».

25. Приказ Минцифры России от 18.08.2021 № 856 «О порядке формирования, актуализации классификатора полномочий и обеспечения доступа к нему» (зарегистрировано в Минюсте России 08.10.2021 № 65350).

26. Приказ Минцифры России от 18.08.2021 № 857 «Об утверждении единых требований к формам доверенностей, необходимых для использования квалифицированной электронной подписи» (зарегистрировано в Минюсте России 08.10.2021 № 65353).

27. Приказ Минцифры России от 18.08.2021 № 858 «Об утверждении единых требований к машиночитаемым формам документов о полномочиях» (зарегистрировано в Минюсте России 08.10.2021 № 65351).

28. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 02.07.2021) «Об электронной подписи» (с изм. и доп., вступ. в силу с 01.03.2022).

29. Постановление Правительства РФ от 15.12.2020 № 2101 «Об утверждении размера финансового обеспечения гражданской ответственности юридического лица, предполагающего оказывать

услуги доверенной третьей стороны, за ущерб, причиненный третьим лицам вследствие оказания таких услуг ненадлежащего качества».

30. Приказ Минкомсвязи России от 11.04.2017 № 187 «Об обеспечении осуществления Министерством связи и массовых коммуникаций Российской Федерации функции доверенной третьей стороны» (вместе с «Положением о доверенной третьей стороне при обмене электронными документами в случаях, если ее участие в таком обмене предусмотрено международными договорами Российской Федерации») (зарегистрировано в Минюсте России 04.05.2017 № 46598).

31. Приказ Минцифры России от 30.11.2020 № 641 «Об утверждении требований к порядку реализации функций аккредитованной доверенной третьей стороны и исполнения ее обязанностей» (зарегистрировано в Минюсте России 23.12.2020 № 61746).

32. Приказ Минцифры России от 30.11.2020 № 642 «Об утверждении Административного регламента предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по аккредитации доверенных третьих сторон и Административного регламента осуществления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственного контроля (надзора) за соблюдением аккредитованными доверенными третьими сторонами требований, которые установлены Федеральным законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами».

33. Приказ ФСБ России от 04.12.2020 № 556 (ред. от 13.04.2021) «Об утверждении Требований к средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи» (зарегистрировано в Минюсте России 30.12.2020 № 61970).

Перспективные СКЗИ в ЭДО Сбербанка. Примеры успешного внедрения облачных сервисов в Сбербанке:

• Облачный сервис неквалифицированной электронной подписи в Сбербанк бизнес-онлайн (УНЭП в СББОЛ) – текущая аудитория – более 320 тысяч пользователей, потенциал – более 800 тысяч.

Например, через месяц после внедрения сервиса один из крупных клиентов Сбербанка смог подписать электронной подписью важный документ с борта ледокола в центре Северного Ледовитого океана.

• Мобильный УКЭП для клиентов внутренней системы Сенат – используется для принятия решения коллегиальных органов руководителей Сбербанка.

• Облачный сервис УНЭП для кадрового ЭДО. Аудитория – более 300 тысяч сотрудников, в потенциале – тиражирование сервиса на процесс приема внешних кандидатов.

• Мобильный УКЭП для клиентов Private Banking – в настоящее время пилотируется на группе из 250 клиентов, в перспективе – 6 тысяч.

Контрольные вопросы

1. Что, согласно закону № 63-ФЗ, требуется для организации защищенного ЭДО?
2. Какой тип электронной подписи приравнивается к собственноручной?
3. В чем основной недостаток реализации ЭДО без СКЗИ?
4. Что сделано в России для борьбы с мошенничеством при использовании электронной подписи в 2021 году?
5. Какие свойства документа, доступные в ЭДО, обеспечиваются электронной подписью?

Тесты для самоконтроля

1. Какие государственные структуры имеют право выдавать сертификаты УКЭП на подведомственной основе? Выберите все правильные ответы.

а) Федеральная налоговая служба
б) Министерство финансов
в) Центральный банк
г) ФСБ

2. Какое утверждение о доверии ложное?

а) доверие всегда транзитивно

б) доверие может быть быстро утрачено

в) шифрование трафика не является источником доверия

г) доверие лежит в основе инфраструктуры открытых ключей

3. Какую из задач помогают решить алгоритмы симметричного шифрования?

а) конфиденциальность

б) доступность

в) аутентичность

г) неотрицание авторства

4. Какой публичный удостоверяющий центр продолжает оказывать услуги без ограничений клиентам из России?

а) Thawte

б) GeoTrust

в) GlobalSign

г) DigiCert

5. Что можно сделать с помощью сервиса badssl.com?

а) отправить на экспертизу образец вредоносного кода

б) протестировать поведение браузера при работе с различными проблемными сертификатами

в) узнать о стойкости современных алгоритмов шифрования и электронной подписи

г) поучаствовать в проекте по взлому протокола TLS

6. Какие элементы формируют доверие к инфраструктуре открытых ключей? Выберите все правильные ответы.

а) удостоверяющий центр

б) платформа PKI

в) криптографические алгоритмы

г) орган, выдающий разрешение на работу УЦ

д) закрытые ключи

е) публичные ключи

ПРАКТИЧЕСКИЕ РАБОТЫ

Практическая работа 1
Симметричное шифрование и дешифрование

Цель – научиться кодировать и декодировать информацию симметричным методом.

Сведения, необходимые для выполнения работы

К методам шифрования с симметричным ключом относятся: методы замены (моноалфавитная, гомофоническая, полигамная и полиалфавитная, например, по матрице Вижинера или модифицированной матрице), методы перестановки (например, по маршрутам Гамильтона или с использованием аппаратных схем), аналитические методы с использованием аналитических преобразований и аддитивные методы гаммирования или с применением генераторов (датчиков) псевдослучайных чисел.

Криптостойкость перечисленных методов шифрования определяется длиной ключа, которая для современных систем должна быть хотя бы 90 бит, но может достигать 1024 бита. Для повышения криптостойкости могут использоваться несколько ключей: зашифрованная с помощью первого ключа информация подвергается шифрованию с помощью второго ключа и т. д.

С этой же целью могут использоваться переменные методы шифрования, когда ключ шифрования используется и для выбора алгоритма шифрования. При симметричном шифровании процесс зашифровывания и расшифровывания использует некоторый секретный ключ.

Обычно реализуются два типа алгоритмов:

- Поточное шифрование (побитовое).
- Блочное шифрование (при шифровании текст предварительно разбивается на блоки, как правило, не менее 64 бит).

Примеры симметричного шифрования: ГОСТ 28147–89, HMAC (алгоритм шифрования, использующий хеш-функцию и закрытый ключ), Blow Fish, HMAC-MD5 (хеш-функция для генерации 128-битной цифровой подписи), IDEA, SHA (хеш-функция для ге-

нерации 160-битной цифровой подписи), DES (использует закрытый ключ и случайное число).

Достоинство симметричного шифрования – скорость выполнения преобразований и относительная легкость внесения изменений в алгоритм шифрования; недостаток – ключ известен получателю и отправителю, что создает проблемы при распространении ключей и доказательстве подлинности сообщения.

Задание

1. Изучить симметричные алгоритмы шифрования.
2. Выбрать один из методов симметричного шифрования.
3. Разработать программу, позволяющую зашифровывать текст этим методом.
4. Проверить выполненные действия расшифрованием.

Вопросы для самоконтроля

1. Что такое гаммирование?
2. Что такое ключ?
3. Сравните наиболее известные методы шифрования.
4. Все ли методы шифрования можно реализовать как программно, так и аппаратно?
5. Распространенным методом криптоанализа является статистический подход. Все ли симметричные методы шифрования нестойки к статистическим методам криптоанализа?
6. Зависимость стойкости симметричного шифра к статистическим методам криптоанализа.

Практическая работа 2
Асимметричное (несимметричное) шифрование и дешифрование

Цель – научиться кодировать и декодировать информацию асимметричным методом.

Сведения, необходимые для выполнения работы

Асимметричное (несимметричное) шифрование – это шифрование с открытым ключом. Информация шифруется с помощью открытого ключа, а расшифровывается с использованием секретного ключа.

В несимметричных алгоритмах шифрования ключи зашифровывания и расшифровывания всегда разные (хотя и связанные между собой). Ключ зашифровывания является несекретным (открытым), ключ расшифровывания – секретным.

Примеры симметричного шифрования: RSA (базовый алгоритм шифрования, предложен Р. Ривестом, Э. Шамиром и Л. Адлманом), Эль-Гамаля (алгоритм использует простое число p, образующую группы g и экспоненту $y = gx(\mathrm{mod}\ p)$), Месси-Омуры (алгоритм использует простое число p, такое что $p - 1$ имеет большой простой делитель в качестве открытого ключа, секретный ключ определяется в процессе диалога между приемником и источником), DSS (алгоритм генерации цифровых подписей), Diffie-Hellman (алгоритм генерации открытого ключа, позволяющий передавать его по открытым линиям по частям).

Недостаток асимметричного шифрования – низкое быстродействие алгоритмов (из-за длины ключа и сложности преобразований); достоинство – применение асимметричных алгоритмов для решения задачи проверки подлинности сообщений, целостности, аутентификации (электронная цифровая подпись), скорость работы, а также секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа.

Привлекательность методов шифрования с использованием открытых ключей заключается в отсутствии необходимости рассылки секретных ключей. Распространение систем с открытыми ключами сдерживается отсутствием доказательств невозможности получения секретных ключей, кроме как путем их полного перебора.

Задание

1. Изучить описанные асимметричные алгоритмы шифрования.
2. Выбрать один из методов асимметричного шифрования.
3. Разработать программу, позволяющую зашифровывать этим методом.
4. Проверить выполненные действия расшифрованием.

Вопросы для самоконтроля

1. Для чего в ассиметричных методах шифрования требуется применить два ключа?
2. Почему именно методы несимметричного шифрования используются при генерации электронной подписи?
3. Сравните алгоритмы системы Эль-Гамаля, криптосистемы Мак-Элиса и RSA.
4. Какой метод несимметричного шифрования требует больших ресурсов ИС?

Практическая работа 3
Особенности систем защиты информации в ведущих странах мира

Цель – изучить элементы конкретных СЗИ в ведущих странах мира.

Сведения, необходимые для выполнения работы

В настоящее время задача по ЗИ – это не только защита сведений (сообщений, данных), независимо от формы их представления, но и комплекс мер, направленных на защиту IT-инфраструктуры, в которой эти сведения хранятся и обрабатываются. Вполне допустимо привести аналогию с домом, в котором хранится и используется имущество его хозяина. В этом случае защите подлежит не только имущество внутри дома, но и сам дом, так как он есть неотъемлемая часть имущества собственника.

Именно поэтому все чаще под термином «ЗИ» подразумевают защиту IT-инфраструктуры в целом. Отсутствие должной защиты IT-инфраструктуры влечет за собой возникновение рисков потери информации. К наиболее распространенным задачам по обеспечению безопасности IT-81 инфраструктуры можно отнести:

- защиту инфраструктуры компании или отдельных ее ресурсов от хакерских атак;
- организацию безопасной передачи информации между филиалами/удаленными офисами или сотрудниками компании по открытым каналам связи;

- разграничение прав доступа к информации среди сотрудников компании. Рынок решений в области обеспечения ИБ предлагает различные средства, решающие те или иные задачи. Естественно, чем более универсальным будет выбранное средство и чем больше задач оно решит, тем лучше.

Централизованное управление – несомненный плюс, характеризующий универсальное средство. Еще одним свойством универсальности можно считать процедуру внедрения средства в существующую IT-инфраструктуру. Здесь основной девиз: как можно меньше изменений, так как изменение может повлечь нарушения в работе.

Помимо требований покупателей к функциональности и универсальности средств ЗИ существуют требования со стороны законодательства. Особое внимание в последнее время уделяется вопросу защиты IT-инфраструктур, в которых хранятся и обрабатываются персональные данные. В соответствии с законом «О персональных данных» в этом случае должны использоваться сертифицированные средства ЗИ.

На основании вышеизложенного можно сформулировать требования к средству ЗИ, наиболее полно и эффективно обеспечивающему безопасность IT-инфраструктуры:

- средство должно как можно более полно решать задачи, связанные с обеспечением IT-инфраструктуры компании;
- процесс внедрения не должен требовать кардинальной перестройки IT-инфраструктуры;
- простота и удобство настройки и управления, наличие механизмов удаленного и централизованного управления;
- сертификация и соответствие требованиям законодательства.

Задание

Описать СЗИ в определенной стране. Охарактеризовать разнообразие органов и служб ЗИ. Рассмотреть особенности защиты персональных данных, государственной и коммерческой тайны в ведущих зарубежных странах.

Страну выбрать по варианту: 1 вариант – США. 2 – Великобритания. 3 – Германия. 4 – Франция. 5 – Япония. 6 – Китай.

7 – Канада. 8 – Швеция. 9 – Россия. 10 – любая из бывших соцстран или бывших республик СССР.

Вопросы для самоконтроля

1. Опишите геополитическое влияние в области ИБ.
2. Поясните теорию, что система защиты не может быть коммерческой.

Практическая работа 4
Формирование электронно-цифровой подписи

Цель – ознакомиться с основами применения электронной цифровой подписи.

Сведения, необходимые для выполнения работы

Термин «цифровая подпись» используется для методов, позволяющих устанавливать подлинность сообщения при возникновении спора относительно его авторства. Применяется в ИС, в которых отсутствует взаимное доверие сторон. Известны два класса формирования цифровой подписи:

1) использует труднообратимые функции типа возведение в степень в конечных полях 82 большой размерности. К этому классу относится ГОСТ РФ. Он является усложнением алгоритмов цифровой подписи RSA и Эль-Гамаля;

2) использует криптостойкие преобразования, зависящие от секретного ключа. Одной из программ ЗИ при помощи системы из двух ключей является программа PGP (Pretty Good Privacy), разработанная в США Филиппом Циммерманом (Philip Zimmermann) в начале 90-х годов. Для проверки электронной подписи в компьютер, с помощью которого выполняется эта проверка, необходимо установить открытый ключ, парный секретному ключу, с помощью которого образуется файл электронной подписи.

Передача открытого ключа идет в три шага:

1. Экспорт ключа в файл. Это выполняется на компьютере подписанта. В окне PGPkeys пометить в списке ключей нужную строку и выбрать пункт меню Export. В окне указывается место в файловой системе, куда будет помещен файл с публичным ключом. По умолчанию его имя совпадает с именем ключа. Создаваемые файлы

имеют расширение .asc. Этот файл пересылается в компьютер, с помощью которого предполагается проверять электронную подпись.

2. Пересылка файла на место проверки подписи. Файлы с расширением .asc помечаются значком. После пометки нужного файла нажимается кнопка Открыть. Пользователь компьютера должен пометить нужные ему ключи и нажать кнопку Import. После этого список ключей в окне PGPkeys дополняется строкой с информацией о новом импортированном ключе. Теперь его можно использовать для проверки электронных подписей.

Для проверки подлинности публичного ключа его отпечаток владельцем пары ключей передается на место его использования и там проверяется.

Для получения отпечатка в окне PGPkeys следует пометить строку нужного ключа и затем выбрать пункт меню Properties. Теперь его можно передавать на место проверки ключа.

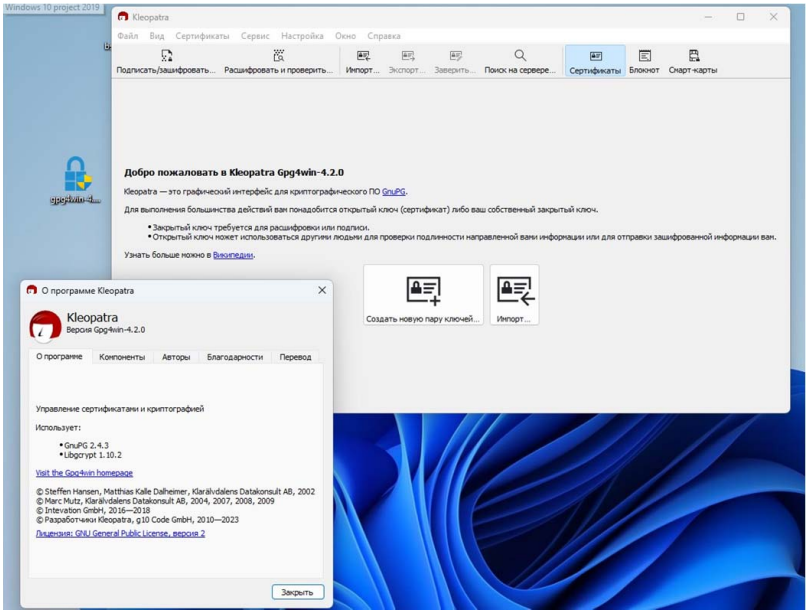
3. Импорт ключа из файла. Для отображения отпечатка имеющегося ключа поступают аналогичным образом и сравнивают полученный извне отпечаток с тем, который высвечивается в окне свойств ключа. В случае их совпадения делается вывод об истинности ключа.

Задание

1. С помощью ПО, основанного на стандарте OpenPGP и соответствующего стандарту RFC 4880 (например, продукта Gpg4win, который можно скачать по ссылке Gpg4win – Download Gpg4win), создать пару ключей, необходимых для создания электронной цифровой подписи.
2. Создать файл с электронной подписью.
3. Осуществить проверку электронной подписи.
4. Осуществить передачу открытого ключа.
5. Осуществить получение и проверку отпечатка публичного ключа.

PGP – Pretty Good Privacy, программа и библиотека функций, позволяющая выполнять операции шифрования, цифровой подписи файлов и других видов информации. Основы проекта заложены Филиппом Циммерманом в 1991 году. Имеет ряд реализации и может быть встроено в стороннее программное обеспечение.

Ниже представлена установка программного продукта Kleopatra как требуемого нам функционального продукта.



Вопросы для самоконтроля

1. Какие существуют группы организационно-технологических мер?
2. Дайте определение целостности данных.
3. Какие принципы использованы при рассмотрении вопроса целостности?
4. Поясните понятие корректности транзакций.
5. В чем заключается идея минимизации привилегий?
6. Что такое цифровая подпись?
7. Какие разработаны классы формирования цифровой подписи?
8. В чем отличие обычной и цифровой подписи?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Журавлёва, Н. А. Экономическая безопасность : учеб. пособие / Н. А. Журавлёва ; Петербургский государственный университет путей сообщения Императора Александра I. – Санкт-Петербург : ФГБОУ ВО ПГУПС, 2022. – 78 с. – URL: e.lanbook.com/book/224522 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-7641-1682-2.
2. Кийко, П. В. Цифровые технологии : учеб. пособие / П. В. Кийко ; Омский государственный аграрный университет имени П.А. Столыпина. – Омск : ФГБОУ ВО Омский ГАУ, 2023. – 108 с. – URL: e.lanbook.com/book/349799 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-907687-34-9.
3. Краковский, Ю. М. Методы защиты информации : учеб. пособие / Ю. М. Краковский. – Изд. 3-е, перераб. – Санкт-Петербург [и др.] : Лань, 2021. – 234 с. – URL: e.lanbook.com/book/156401 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8114-5632-1.
4. Надёжность и защита информации автоматизированных систем : учеб. пособие / М. Н. Краснянский, В. Г. Матвейкин, А. В. Затонский [и др.] ; Тамбовский государственный технический университет. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2022. – 95 с. – URL: e.lanbook.com/book/355145 (дата обращения: 15.01.2024). – Режим доступа: по подписке. – ISBN 978-5-8265-2460-2.
5. Искусственный интеллект и машинное обучение в кибербезопасности : учеб.-метод. пособие / сост.: О. И. Шелухин, А. В. Осин, Д. И. Раковский. – Москва : Московский технический университет связи и информатики, 2022. – 52 с. – URL: e.lanbook.com/book/333755 (дата обращения: 15.01.2024). – Режим доступа: по подписке.
6. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности / Н. Ш. Козлова, N. S. Kozlova, В. А. Довгаль, V. A. Dovgal // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и техниче-

ские науки. – 2023. – № 3 (326). – С. 65-72. – ISSN 2410-3225. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/journal/issue/347516 (дата обращения: 24.01.2024). – Режим доступа: для авториз. пользователей.
7. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. – Пермь : ПНИПУ, 2023. – 91 с. – ISBN 978-5-398-02866-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/328889 (дата обращения: 24.01.2024). – Режим доступа: для авториз. пользователей.
8. AI-Russia : открытая библиотека кейсов и премия в области бизнес-эффективности проектов, созданных с использованием искусственного интеллекта : [сайт] / Альянс в сфере искусственного интеллекта. – URL: ai-russia.ru (дата обращения: 24.01.2024).

ГЛОССАРИЙ

Архивация данных – способ хранения информации, который позволяет не потерять данные в случае выхода из строя оборудования либо при попытке случайного или преднамеренного удаления.

Беспарольная аутентификация – способ идентификации пользователей, который позволяет отказаться от паролей и выполнять ее с помощью других методов: через привязанное мобильное устройство, аппаратный ключ, биометрические данные и т. д. Беспарольная аутентификация более безопасна, поскольку её весьма затруднительно произвести без личного присутствия пользователя, а также более удобна, поскольку не нужно менять пароль каждые *n* дней.

Защита конечных устройств от атак нулевого дня – любой софт, может иметь уязвимости. Зачастую они исправляются до того, как станут публичными, но бывают ситуации, когда между появлением вредоносных приложений, которые используют уязвимости, и выходом патча может пройти несколько дней. Данные о такого типа уязвимостях называются атаками нулевого дня. Обеспечить защиту рабочих станций от них могут помочь технические средства, например, модуль Vulnerability Assessment сервиса Microsoft Defender for Endpoint. Он сообщит об уязвимостях и серверах, на которых присутствует уязвимое ПО, а также программных поправках (патчах), которые нужно установить.

Защита от атак вирусов-шифровальщиков – вирус-шифровальщик – способ проникновения в систему, с помощью которого злоумышленники не только шифруют документы, но и архивы, а также удаляют теневые копии. Чтобы обезопасить себя, пользователи могут автоматически сохранять копии в облаке. Все предыдущие версии документов также будут сохраняться. Если файлы были зашифрованы или удалены – они будут восстановлены, сколько бы изменений в них ни сделали.

Защита от атак на мобильные устройства – основная угроза, связанная с мобильными устройствами, следующая: устройства личные, а информация на них может быть и корпоративной. Если сотрудники компании работают с мобильных телефонов с корпоративной почтой или документами, вы должны иметь возможность защитить данные, принадлежащие компании. Подключение мобильных телефонов к сервису MEM (Microsoft endpoint manager) даст возможность настроить телефоны сотрудников более безопасно, а также удалить рабочие данные при увольнении сотрудника или в случае кражи и потери устройства.

Защита от вирусов – лучшим способом защиты от вирусов является антивирус. Он обязательно должен быть у каждого. Именно поэтому операционные системы Windows 10 и Windows 11 имеют встроенный и бесплатный антивирус.

Защита от вредоносных вложений – вредоносные вложения электронной почты – одна из наиболее распространенных угроз. Например, это могут быть макросы, которые передают данные с вашего ноутбука или шифруют другие документы. Внешне они могут быть идентичны с обычными файлами. Поэтому для обеспечения защиты пользователей электронная почта от Microsoft автоматически тестирует поведение документов до того, как письмо попадет в почтовый ящик. Если поведение похоже на подозрительное, то письмо будет доставлено без вложения.

Защита от вредоносных ссылок в электронной почте – для получения несанкционированного доступа хакеры могут рассылать письма, содержащие вредоносные ссылки, похожие, например, на настоящие сайты банков, и переход по ним может закончиться скачиванием вируса, потерей доступа к банку, площадке для торгов и т. д. В связи с этим существуют способы автоматизированной защиты, которые позволяют проверять каждый переход по ссылке из электронного письма или документа в момент клика по ней. Если ссылка ведет на вредоносный сайт, то переход будет заблокирован.

Защита от утечки документов – технология для защиты документов путем их шифрования и назначения прав на доступ к ним другим пользователям, например, Azure Information Protection. Они позволяют обеспечить безопасность в случае утечки документов за пределы организации.

Защита серверов на базе разных операционных систем – в большинстве компаний используются различные операционные системы, и зачастую они отличаются от тех ОС, которые установлены на рабочих станциях. Приложения, базы данных, контейнеры в основном работают на ОС Linux. При этом встроенная защита на Linux весьма ограничена. Обеспечить защиту от уязвимостей могут помочь решения класса Endpoint Detection & Response (EDR), которые предоставляют в облако для анализа информацию о процессах, и если файлы или поведение пользователя подозрительны, они будут заблокированы.

Компрометация учетной записи – доступ к почтовым ящикам, данным и различным службам контролируется с помощью учетных данных, например, имени пользователя и пароля или ПИН-кода. Если кто-то посторонний украдет эти учетные данные, они считаются скомпрометированными. Имея их, злоумышленник может войти в почтовый ящик или службу как настоящий пользователь и совершить незаконные действия, например, отправлять электронные письма от имени настоящего пользователя получателям в организации и за ее пределами. Когда происходит отправка данных по электронной почте внешним получателям, имеет место их утечка, что может представлять серьезные риски. В связи с этим необходимо уделять внимание защите учетных записей, например, использовать многофакторную идентификацию пользователей при запросе доступа к данным.

Компрометация привилегированного пользователя – использование ИТ-администраторами одного аккаунта с большим количеством привилегий может повлечь серьезные угрозы для безопасности организации в случае его компрометации. Именно поэтому им необходимо иметь несколько учетных записей с разными полномочиями, например, аккаунт без привилегии для работы в Интернете, аккаунт для администрирования рабочей станции, аккаунт для администрирования сервера, аккаунт для администрирования домена и т. д. При таком подходе даже в случае компрометации одного из них злоумышленник не получит всех привилегий.

Классификация конфиденциальной информации – компании хранят множество данных на разных ресурсах, в разных форматах: портал, электронная почта, файловые серверы, базы данных и т. д. Сотрудники далеко не все осознают уровень конфиденциальности данных, что может привести к их утечке и репутационным и финансовым рискам. Для обеспечения защиты информации необходимо классифицировать данные – часть из них можно классифицировать автоматически с помощью различных сервисов, а оставшаяся должна быть классифицирована сотрудниками. В этом случае к ним можно применить настройки защиты от утечки в соответствии с классификацией.

Многофакторная аутентификация – способ дополнительной проверки пользователей, например, с помощью телефонного звонка, смс, подтверждения в мобильном приложении или ввода цифр из мобильного приложения. Современные технологии предлагают возможность гибкой настройки, например, не требовать второй

фактор при работе с IP-адреса компании, но требовать при работе из дома.

Облачный SOC (Security operations center) – в любой компании, особенно крупной, существует ряд систем, слабо связанных друг с другом: разные системы аутентификации, разные менеджеры, администраторы и т. д. Это подразделения, занимающиеся вопросами безопасности на организационном и техническом уровне, которые работают на успешное отслеживание и отражение атак, а при необходимости оперативно помогают устранять их последствия. Существуют провайдеры, которые предоставляют данную услугу с помощью облака, что значительно упрощает жизнь заказчика, поскольку им не нужно самостоятельно строить SOC внутри своей ИТ-инфраструктуры.

Предотвращение несанкционированного доступа из недоверенных локаций – зачастую хакеры, стараясь остаться анонимными, скрывают своё местоположение, поэтому одним из способов защиты является ограничение входа с недоверенных геолокаций. Например, ИТ-департамент может составить списки локаций, через которые может быть предоставлен доступ, на основе публичных IP-адресов или соответствующих им геолокаций, чтобы обеспечить защиту данных.

Соответствие требованиям регуляторов – комплексный процесс, который выходит за пределы компетенций одного лишь ИТ-департамента. Одно из наиболее важных требований – сохранение информации от случайного или целенаправленного удаления. Для этого необходимо продумать внутри компании политики сохранения данных, которые защитят важные документы, письма и даже сообщения в чате от случайного или целенаправленного удаления в течение выбранного периода.

Физическая безопасность дата-центров – безопасность инфраструктуры складывается из ряда факторов, в том числе безопасности физической. Когда оборудование находится на территории компании, организовать физическую безопасность бывает сложно, потому что необходимо учесть ряд важных факторов. Поэтому небольшие компании, как правило, самостоятельно не могут позволить себе такой уровень безопасности. В специализированных дата-центрах работают системы контроля доступа, пропускной режим, круглосуточное видеонаблюдение и охрана, доступ третьих лиц затруднен или практически невозможен.

DLP-системы – дополнительную защиту от утечки данных могут обеспечить системы DLP, которые позволяют настроить политики безопасности, чтобы запретить ряд действий с конфиденциальной информацией, например, пересылку за пределы компании или скачивание на локальный ПК. Администратор также будет уведомлен о попытках пользователей выполнить запрещенные действия. Функция DLP доступна не только для электронной почты и хранилищ Sharepoint/Onedrive for Business, но и Microsoft Teams.

UBA (User Behavior Analysis) системы – система UBA выполняет последовательное изучение ряда поведенческих признаков сотрудников: в какое время работает, на какие устройства заходит, к каким файлам получает доступ, в каких группах состоит и т. д. После построения поведенческого профиля пользователя система может сообщать об аномалиях в поведении, которые позволяют выявлять злоумышленников, скомпрометировавших учетную запись пользователя.