DOI 10.36622/VSTU.2023.26.2.010
УДК 004.056.57

СЕТЕВЫЕ АТАКИ НА УРОВНЕ ПРИЛОЖЕНИЙ: РИСК-ЛАНДШАФТ И ЧАСТНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

С.А. Хромых, Г.А. Остапенко, Д.В. Щербакова, А.А. Остапенко

Рассмотрена проблема сетевых атак на уровне приложений, и обосновывается её актуальность. Приведены векторы и уязвимости сетевых атак на уровне приложений. Описана и реализована методика риск-оценки на основе данных по атакам и уязвимостям в 2022 году. Построены матрица уязвимостей и риск-ландшафт по данным риск-оценок в указанном периоде. На основе риск-ландшафта проведена оценка степени опасности векторов атак и уязвимостей. Выделены наиболее опасные сочетания векторов и уязвимостей. Для таких сочетаний предложены соответствующие фрагменты частной политики защиты информации. Акцентируется внимание на важности разработки частных политик безопасности информации, учитывающих особенности деятельности конкретных предприятий для более эффективной защиты от атак на уровне приложений и не только.

Ключевые слова: корпоративная сеть, векторы атаки, уязвимости, риск-ландшафт, частная политика.

Введение

Сегодня большинство компаний опираются на корпоративные сети, которые представляют собой совокупность программно-технический и людских ресурсов. Для управления технологическими процессами персоналу требуются соответствующие инструменты. В роли таких инструментов выступают программы и приложения, являющиеся частью программно-технического комплекса. Таким образом, защита корпоративных сетей (КС) на уровне приложений является одним из ключевых аспектов обеспечения информационной безопасности КС. Пренебрежение защитой приложений может привести к серьезным последствиям, например, к утечке конфиденциальной информации и нарушению её бизнес-процессов [1-10].

Актуальность данной темы обуславливается, также, постоянным ростом числа компаний, использующих КС для оптимизации своих бизнес-процессов, и, как следствие, ростом числа сетевых атак, в том числе, на приложения. В связи с этим существует необходимость разработки более эффективных методов обеспечения информационной безопасности КС, основанных на оценке, прогнозировании и регулировании рисков успешности сетевых атак на уровне приложений.

Очевидно, что организации разрабатывают или используют приложения для реализации бизнес-процессов. Чем больше компаний так или иначе будут задействовать в своей работе приложения, тем больше злоумышленников будут пытаться проводить сетевые атаки с целью получения выгоды.

Стоит понимать, что часть компаний задействуют приложения только для внутренних процессов своей работы. Однако множество компаний (чаще всего из сферы услуг) используют приложения для реализации своих товаров и услуг, и они становятся мишенью для злоумышленников. Главной проблемой таких приложений является прямой доступ к базам данных клиентов. Поэтому неудивительно, что такие компании часто становятся объектами атак.

По этой причине переход компаний в виртуальное пространство создает необходимость разработки все более совершенных политик, регламентов и инструкций по защите информации [1-2].

Для этого требуется проведение исследований в области защиты информации, где необходимо описать наиболее опасные векторы атак и уязвимости на уровне приложений. Полученные данные стоит систематизировать для дальнейшего анализа

и формирования на основе этих результатов вышеупомянутых политик, регламентов и инструкций.

Риск-анализ сочетаний векторов и уязвимостей позволит получить адекватную картину безопасности, а также даст возможность целенаправленно совершенствовать организационно-правовые документы и успешно бороться с растущим числом сетевых атак не только на уровне приложений, но и во всем поле реализуемых злоумышленниками сценариев нападений.

Риск-ландшафт уязвимостей и векторов атак на уровне приложений

Объектом исследования являются КС и информационные технологии, применяемые в компаниях.

Предметом исследования являются методы совершенствования организационно-правового обеспечения информационной безопасности КС на основе оценки, прогнозирования и регулирования рисков успешности сетевых атак на уровне приложений.

Целью исследования является повышение информационной защищенности КС предприятий за счет выявления наиболее опасных сочетаний векторов атак и уязвимостей, и построение им адекватной подсистемы обеспечения безопасности.

Для достижения поставленной цели необходимо решить следующие задачи:

1) с использованием интернет-пространства и других информационных источников аккумулировать данные и знания о защите, уязвимостях, сценариях и ущербах, относящиеся к атакам на уровне приложений, необходимые и достаточные для последующего риск-анализа.

2) оценка риска успешности атак на уровне приложений на КС с учетом статистики накопленной базы данных.

3) с учетом проведенного риск-анализа и построенного риск-ландшафта создание частной политики защиты информации, отвечающей требованиям действующих стандартов безопасности.

Существует множество способов атаки на приложения, которые формируют векторы (сценарии) атаки, приводящие ко взлому защиты и дальнейшим отрицательным последствиям для объекта атаки. В данной работе объектом атаки будет являться корпоративная сеть.

Различные источники предлагают разную классификацию векторов атак: так, например, Antihacking.ru выделяет четыре вектора атаки [1], а ресурс habr.com делит все атаки всего на два типа [2], также многие сайты классифицируют вектора атак, опираясь на наиболее популярные категории уязвимостей. Однако, используя ресурс capec.mitre.org [3] в отношении атак на приложения можно выделить 6 сценариев, представленных в табл. 1.

Таблица 1

Векторы атак на приложения [3]

Вектор атаки	Описание	Шаблоны атак
Va_1 Управление общими ресурсами	Злоумышленник атакует ресурс, совместно используемый несколькими приложениями, пулом приложений или мультиплексированием аппаратных выводов, чтобы влиять на поведение. Если злоумышленник может манипулировать этим общим ресурсом, то другие приложения или потоки, использующие общий ресурс, часто будут продолжать доверять действительности скомпрометированного общего ресурса и использовать его в своих вычислениях. Это может привести к неверным предположениям о доверии, повреждению дополнительных данных в результате обычных операций других пользователей общего ресурса.	Использование временного выполнения инструкций

Продолжение табл. 1

Вектор атаки	Описание	Шаблоны атак
Va_2 Обход аутентификации	Злоумышленник получает доступ к приложению, службе или устройству с привилегиями авторизованного или привилегированного пользователя, обходя механизм аутентификации. Таким образом, злоумышленник может получить доступ к защищенным данным без аутентификации.	Принудительный просмотр
		Подделка подписи API веб-сервисов с использованием слабости расширения хеш-функции
		Выход из виртуализации
		Подделка запроса на стороне сервиса
		Ключевое согласование атаки Bluetooth (KNOB)
Va_3 Внедрение кода	Злоумышленник использует уязвимость в проверке ввода на цели, чтобы внедрить новый код в тот, который в данный момент выполняется.	Внедрение SQL-кода
		Внедрение содержимого файла
		Использование метасимволов в заголовках электронной почты для внедрения вредоносных нагрузок
		Межсайтовый скриптинг (XSS)
		Общая кросс-браузерная меж-доменная кража
Va_4 Повышение привилегий	Злоумышленник использует уязвимость, позволяющую ему повысить свои привилегии и выполнить действие, на выполнение которого он не должен иметь права.	Перехват привилегированного потока выполнения
		Подрывные средства подписи кода
		Целевые программы с повышенными привилегиями
		Межзональные сценарии
		Перехват привилегированного процесса

Окончание табл. 1

Вектор атаки	Описание	Шаблоны атак
Va_5 Препятствие взаимодействию	Злоумышленник препятствует взаимодействию между компонентами системы. Прервав или отключив эти взаимодействия, злоумышленник часто может перевести систему в деградированное состояние или заставить систему перестать работать должным образом. Это может привести к тому, что компоненты системы будут недоступны, пока препятствие не будет устранено.	Физическое уничтожение ресурса или компонента
		Отключение маршрута
		Глушение сигнала
		Блокировка ресурса

По данным исследования Positive Technologies [5] в 2020-2021 годах 17% атак пришлось на эксплуатацию уязвимостей веб-приложений. 98% всех приложений подвержены атакам, 91% веб-приложений был подвержен утечке данных, а 84% имеют возможность несанкционированного доступа. А наиболее опасными уязвимостями стали недостатки аутентификации и авторизации пользователей. Для дальнейших расчетов будет использоваться DataSet «UNSW-NB15», предоставленный Австралийским центром кибербезопасности (ACCS) [4]. Данный DataSet предоставляет данные не только по атакам на уровне приложений. В него входят также данные, по другим сетевым атакам. Также в нем все атаки распределены по стандартной классификации атак, поэтому данные DataSet будут отсортированы с учетом требуемых параметров (рис. 1).

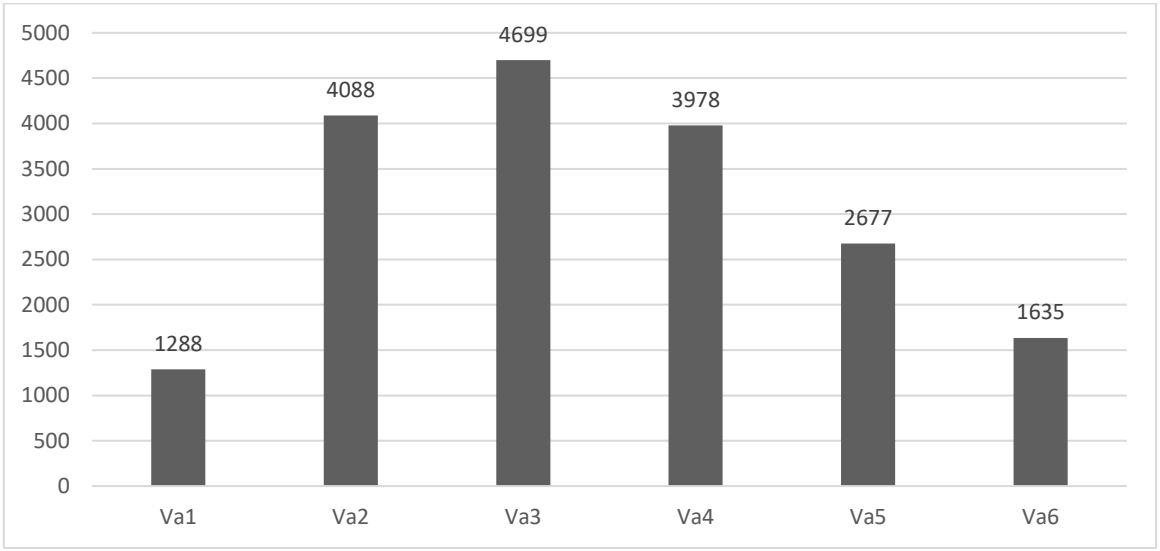

Рис. 1. Число атак по векторам из DataSet «UNSW-NB15» [4]

В данной работе рассмотрены уязвимости и векторы атак, представленные в табл. 1 и 2. Отбор уязвимостей производится с учетом векторов атак (табл. 1), а также с учетом популярности данных уязвимостей на основе статистики БДУ ФСТЭК [8].

Информация по уязвимостям предоставлена ресурсом cwe.mitre.org [6].

Таблица 2

Уязвимости приложений [6]

Название уязвимости	Описание	Код CWE
Неограниченная загрузка файлов с опасным типом	Дает возможность загружать и передавать данные.	CWE-434
Неправильная нейтрализация ввода во время генерации веб-страниц	Не исправляет ввод запроса клиента на веб-страницу другим клиентом.	CWE-79
Неправильная нейтрализация специальных элементов, используемых в команде SQL	Неправильно создается код или его часть, при этом данный сегмент не исправляется в SQL-запросе нижестоящем клиенту.	CWE-89
Неправильное управление привилегиями	Неправильно назначает привилегии для субъекта.	CWE-269
Недостаточно защищенные учетные данные	Использует небезопасный метод хранения учетных данных.	CWE-522
Неправильная авторизация	Неправильная проверка авторизации.	CWE-285
Неконтролируемое потребление ресурсов	Неправильное распределение доступных ресурсов.	CWE-400
Раскрытие конфиденциальной информации	Раскрытие информации субъекту, не имеющему полномочий на доступ к данной информации.	CWE-200
Подделка межсайтовых запросов	Невозможность достоверно проверить запрос, предоставленный пользователем.	CWE-352
Неправильный контроль генерации кода	Входные данные, измененные злоумышленником для генерации кода, не проверяются и не нейтрализуются.	CWE-94

На основе данных БДУ ФСТЭК на рис. 2 представлено число упоминаний уязвимостей из табл. 2. Данные взяты за 2022 год, когда общее число упоминаний уязвимостей составило 5359 [8].

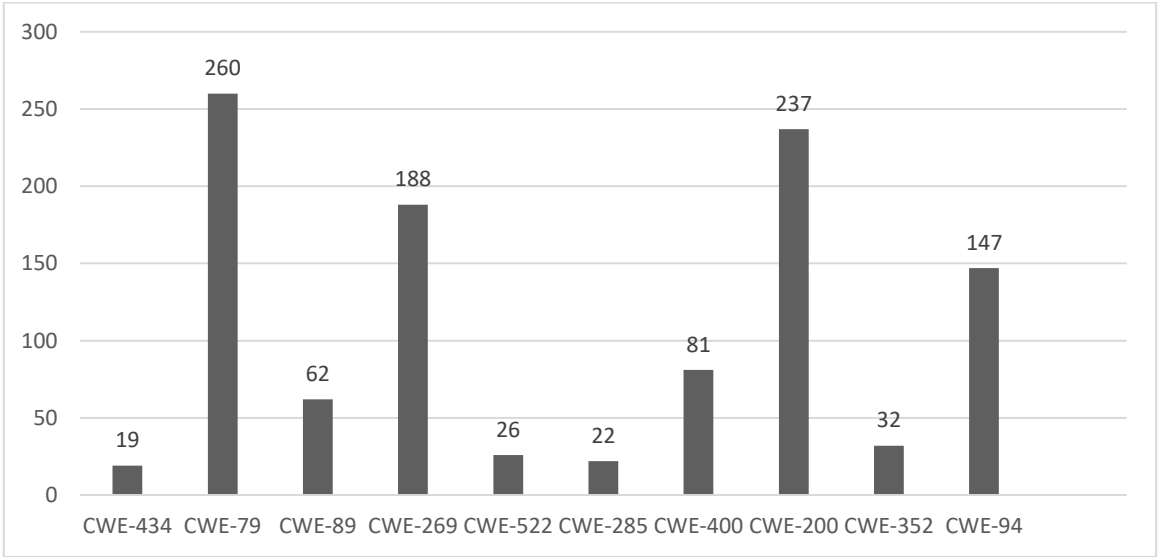

Рис. 2. Число упоминаний уязвимостей в 2022 году [8]

Самыми опасными уязвимостями являются те, что связаны с ошибками авторизации, хранением данных и внедрением кода (рис. 2).

Риск рассчитаем по формуле:

$$\overline{Risk_{sij}} = F_{sij} \times \overline{U_{sij}}, \quad (1)$$

где F_{sij} – частота успешного использования j-ой уязвимости при реализации атаки типа S посредством i-го вектора;

$\overline{U_{sij}}$ – ущерб от реализации атаки типа S посредством i-го вектора.

Частота успешного использования уязвимости находится, как отношение числа упоминания данной уязвимости к общему количеству упоминаний всех уязвимостей за исследуемый период.

Ущерб от реализации атаки рассчитаем в нормированном виде:

$$\overline{U_{sij}} = \frac{\Delta t_{si}}{\max[\Delta t]}, \quad (2)$$

где Δt_{si} – среднестатистическое значение простоя атакуемой сети в результате успеха атаки типа S посредством i-го вектора;

$\max[\Delta t]$ – максимальное значение Δt_{si}.

Представим данные рис. 2 в виде табл. 3.

Представим данные из DataSet «UNSW-NB15» [4] по времени простоя в виде табл. 4, при этом $\max[\Delta t] = 0{,}025$.

Рассчитаем F_{sij} и $\overline{U_{sij}}$, используя данные табл. 3 и 4, а также формулу (2) и занесем полученные значения в табл. 5 и 6.

Таблица 3

Число упоминаний уязвимостей за 2022 год [8]

Уязвимость	Количество упоминаний
CWE-434	19
CWE-79	260
CWE-89	62
CWE-269	188
CWE-522	26
CWE-285	22
CWE-400	81
CWE-200	237
CWE-352	32
CWE-94	147
Общее число упоминаний уязвимостей:	5359

Таблица 4

Среднестатистическое время простоя для каждого вектора атаки [4]

Вектор атаки	Δt_{si}
Va_1	0,008
Va_2	0,005
Va_3	0,006
Va_4	0,005
Va_5	0,002

Таблица 5

Значения F_{sij} для уязвимостей ($\times 10^{-3}$)

Уязвимость	F_{sij}
CWE-434	3,55
CWE-79	48,52
CWE-89	11,57
CWE-269	35,08
CWE-522	4,85
CWE-285	4,11
CWE-400	15,11
CWE-200	44,22
CWE-352	5,97
CWE-94	27,43

Таблица 6

Значения $\overline{U_{sij}}$ для векторов атак

Вектор атаки	$\overline{U_{sij}}$
Va_1	0,32
Va_2	0,2
Va_3	0,24
Va_4	0,2
Va_5	0,08

Для формирования риск-ландшафта нужно построить матрицу смежности векторов атак и уязвимостей. Матрица смежности строится с учетом данных атак на уязвимости и последствий от них, предоставленных ресурсом cwe.mitre.org [6].

На основе данных табл. 5 и 6, а также с учетом табл. 7 и с помощью формулы (1) построим матрицу рисков реализации атак через уязвимости (табл. 8).

Таблица 7

Матрица смежности векторов атак и уязвимостей

	CWE-434	CWE-79	CWE-89	CWE-269	CWE-522	CWE-285	CWE-400	CWE-200	CWE-352	CWE-94
Va_1	1	1	0	0	0	0	1	0	0	0
Va_2	0	0	1	1	1	1	0	0	1	1
Va_3	1	1	1	0	0	0	1	1	0	1
Va_4	0	0	1	1	1	1	0	0	1	1
Va_5	1	1	0	0	0	0	1	0	0	0

Таблица 8

Матрица рисков реализации атак через уязвимости ($\times 10^{-4}$)

	CWE-434	CWE-79	CWE-89	CWE-269	CWE-522	CWE-285	CWE-400	CWE-200	CWE-352	CWE-94
Va_1	1,136	15,526	0	0	0	0	4,835	0	0	0
Va_2	0	0	2,314	7,016	0,97	0,822	0	0	1,194	5,486
Va_3	0,852	11,645	2,777	0	0	0	3,626	10,613	0	6,583
Va_4	0	0	2,314	7,016	0,97	0,822	0	0	1,194	5,486
Va_5	0,284	3,882	0	0	0	0	1,209	0	0	0

На основе табл. 8 построим риск-ландшафт реализации кибератак (рис. 3).

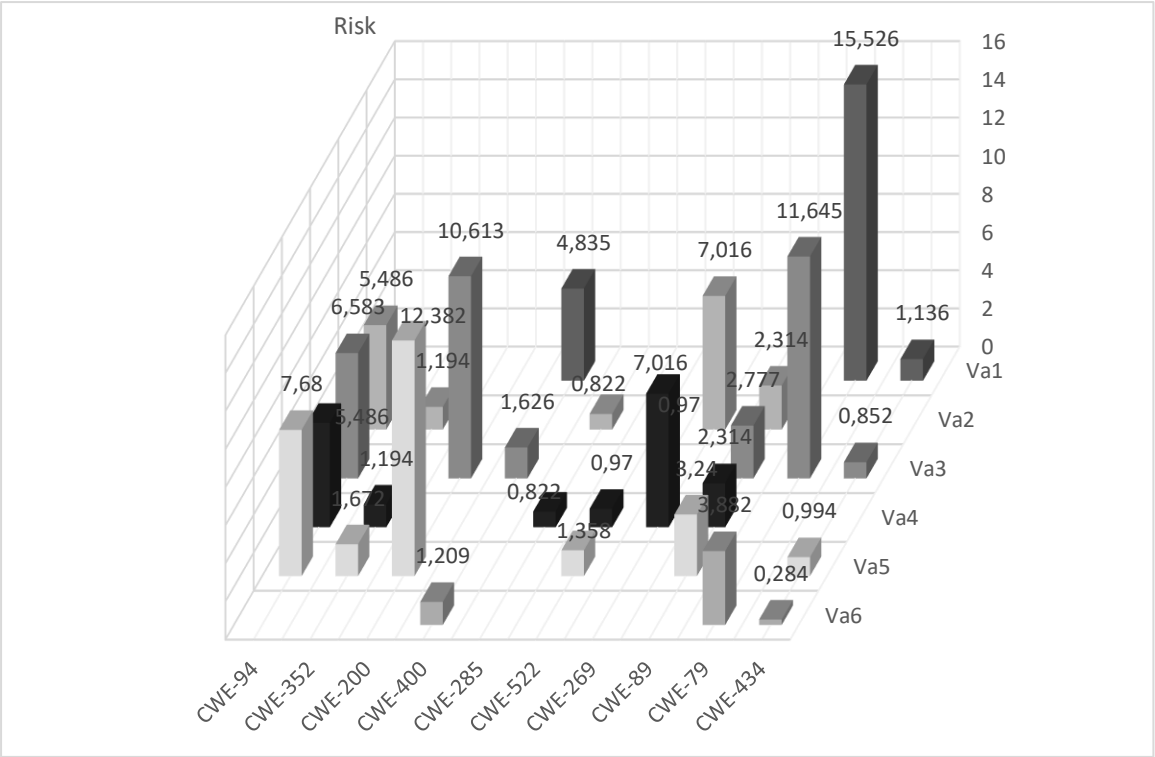

Рис. 3. Риск-ландшафт реализации кибератак ($\times 10^{-4}$)

На основе рис. 3 и табл. 8 получим опасные сочетания уязвимостей и векторов атак.

Таблица 9

Опасные сочетания уязвимостей и векторов атаки

Вектор атаки	Уязвимость
Управление общими ресурсами (Va_1)	Неправильная нейтрализация ввода во время генерации веб-страниц (CWE-79)
	Неконтролируемое потребление ресурсов (CWE-400)
	Неограниченная загрузка файлов с опасным типом (CWE-434)
Обход аутентификации (Va_2)	Неправильное управление привилегиями (CWE-269)
	Неправильный контроль генерации кода (CWE-94)
	Неправильная нейтрализация специальных элементов, используемых в команде SQL (CWE-89)
	Подделка межсайтовых запросов (CWE-352)
	Недостаточно защищенные учетные данные (CWE-522)
Внедрение кода (Va_3)	Неправильная нейтрализация ввода во время генерации веб-страниц (CWE-79)
	Раскрытие конфиденциальной информации (CWE-200)
	Неправильный контроль генерации кода (CWE-94)
	Неконтролируемое потребление ресурсов (CWE-400)
	Неправильная нейтрализация специальных элементов, используемых в команде SQL (CWE-89)
Повышение привилегий (Va_4)	Неправильное управление привилегиями (CWE-269)
	Неправильный контроль генерации кода (CWE-94)
	Неправильная нейтрализация специальных элементов, используемых в команде SQL (CWE-89)
	Подделка межсайтовых запросов (CWE-352)

Продолжение табл. 9

Вектор атаки	Уязвимость
Препятствие взаимодействию (Va_5)	Неправильная нейтрализация ввода во время генерации веб-страниц (CWE-79)
	Неконтролируемое потребление ресурсов (CWE-400)

Из табл. 9 можно сделать вывод, что атаки, направленные на кражу конфиденциальных данных, получение доступа высокого уровня, внедрение вредоносного кода, а также применение мощностей жертв для других операций, являются наиболее частыми и опасными среди всего множества атак.

Наименее опасные сочетания в дальнейшем учитываться не будут, их риски считаются пренебрежимо малыми.

Специфика частной политики безопасности предприятия

Сегодня все предприятия крупного и даже среднего бизнеса создают собственные политики обеспечения безопасности. Очевидно, что корпоративные документы опираются на российские и международные стандарты и ГОСТы в сфере обеспечения информационной безопасности. Например: ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» [9], ISO/IEC 27001 [10] и т.д.

Стоит обратить внимание, что некоторые организации берут за основу своей политики безопасности документы других компаний, и, частично их доработав, утверждают и начинают применять в практике. Данный подход опасен тем, что из-за изначальной направленности на другое предприятие в новой компании такие документы часто создают несостыковки или противоречия при работе.

Такой подход является угрозой, так как он затрудняет работу и документооборот, а также создает юридические лазейки, эксплуатируемые злоумышленниками. Данную проблему стоит упомянуть, однако оценить риски здесь сложно, так как информация по таким инцидентам отсутствует.

В рамках обеспечения информационной безопасности объекты защиты в организации от сетевой атаки на уровне приложений представлены в табл. 10.

Таблица 10

Объекты защиты

Идентификатор объекта защиты	Сценарий атаки	Объект защиты
O_1	Va_1	Автоматизированное рабочее место
O_2	Va_2	Файловая система
O_3	Va_3	Программное обеспечение (ПО)
O_4	Va_4	Операционная система
O_5	Va_5	Персональные мобильные устройства
O_6	Va_6	Серверное оборудование

Для представления плана мероприятий и эффективной системы мер, отвечающих за контроль выполнения требований, определенных частной политикой безопасности, необходимо представить модель нарушителя (табл. 11) и организационную структуру системы обеспечения информационной безопасности организации (табл.12).

Таблица 11

Модель нарушителя

Идентификатор нарушителя	Способ реализации		Тип нарушителя	Мотивация и цели нарушителя
	Сценарий атаки	Уязвимость		
M_1	Va_1	CWE-400	Нарушитель, специализирующийся на взломе систем и сетей	Цель нарушителя – получить доступ к ресурсам организации, чтобы использовать их как основу для дальнейших действий
	Используя ресурсы в своих целях, злоумышленник может проводить другие атаки, при этом не прибегая к собственным мощностям. Для этого используются уязвимости ресурсов системы			
M_2	Va_2	CWE-269	Нарушитель, использующий компьютеры и сети для совершения различных преступлений	Цель нарушителя – получить доступ к файлам организации, чтобы получить выгоду из конфиденциальной информации
	Обходя аутентификацию программного обеспечения, злоумышленник может получить доступ к файлам, содержащим конфиденциальную информацию. Для этого эксплуатируются уязвимости контроля доступа			
M_3	Va_3	CWE-79	Нарушитель, специализирующийся на взломе систем и сетей	Цель нарушителя – внедрить вредоносный код в программное обеспечение организации, чтобы использовать лазейку в своих целях
	Внедряя код в приложения, злоумышленник вносит вредоносное программное обеспечение в системы организации. Для этого используются уязвимости ввода данных			
M_4	Va_4	CWE-269	Нарушитель, использующий компьютеры и сети для совершения различных преступлений	Цель нарушителя – получить доступ к файлам организации, чтобы получить выгоду из конфиденциальной информации
	Повышая привилегии, злоумышленник получает доступ к более конфиденциальным данным и ресурсам организации. Для этого используются уязвимости контроля доступа			
M_5	Va_5	CWE-400	Нарушитель, специализирующийся на взломе систем и сетей	Цель нарушителя – нанести ущерб организации, вызванный нарушением работы ее систем
	Препятствуя взаимодействию компонентов организации, злоумышленник может нарушить работу организации. Для этого используются уязвимости ресурсов системы			

Таблица 12

Организационная структура системы обеспечения информационной безопасности организации

Сценарии атаки	Должностные лица	
	Администратор безопасности	Системный администратор
Va_1	Должен контролировать использование мощностных ресурсов организации и выявлять соответствующие аномалии	Должен устанавливать обновления для устранения уязвимостей, приводящих к компрометации ресурсов
Va_2	Должен контролировать распределение доступа между пользователями	Должен проводить установку обновлений для устранения уязвимостей контроля доступа
Va_3	Должен контролировать приложения на предмет заражения вредоносным ПО	Должен проводить установку обновлений для устранения уязвимостей, приводящих к заражению ПО
Va_4	Должен контролировать распределение доступа между пользователями	Должен проводить установку обновлений для устранения уязвимостей контроля доступа
Va_5	Должен контролировать использование мощностных ресурсов организации и выявлять соответствующие аномалии	Должен устанавливать обновления для устранения уязвимостей, приводящих к компрометации ресурсов

С учетом табл. 11 и 12 возможно приведение мероприятий и мер безопасности в рамках противодействия сетевым атакам на уровне приложений (табл. 13), а также мер контроля (табл. 14).

Таблица 13

Перечень мероприятий по обеспечению безопасности организации при сетевой атаке на уровне приложений

Мероприятие	Объекты защиты	План мероприятий
Защита программного обеспечения	ПО (O_3) Операционная система (O_4)	– Установка и регулярное обновление антивирусных программ, чтобы предотвратить заражение вредоносными программами. – Использование программ брандмауэра для блокировки входящих соединений и предотвращения несанкционированного доступа к системе. – Регулярное обновление ПО и операционных систем, чтобы исправлять уязвимости безопасности и предотвращать атаки. – Ограничение прав доступа пользователей к файлам и папкам, чтобы предотвратить несанкционированный доступ к конфиденциальной информации. – Установка системы мониторинга для обнаружения любых попыток несанкционированного доступа или других вредоносных действий. – Использование шифрования, чтобы защитить конфиденциальные данные от несанкционированного доступа. – Удаление старых и неиспользуемых данных, чтобы предотвратить возможность их несанкционированного использования

Продолжение табл. 13

		– Регулярная проверка целостности файлов, чтобы обнаружить любые изменения, внесенные без разрешения.
Защита баз данных	База данных (O_1)	– Установка соответствующей системы авторизации и аутентификации для ограничения доступа к базе данных только уполномоченным пользователям. – Регулярное создание резервных копий баз данных для обеспечения возможности быстрого восстановления в случае сбоя или потери данных. – Использование шифрования для защиты конфиденциальных данных от несанкционированного доступа. – Установка системы мониторинга для обнаружения любых попыток несанкционированного доступа или других вредоносных действий. – Регулярное обновление программного обеспечения базы данных, чтобы исправлять уязвимости безопасности и предотвращать атаки. – Регулярная проверка целостности данных для обнаружения любых изменений, внесенных без разрешения. – Создание планов для обеспечения возможности быстрого восстановления работы базы данных после кибератак.
Повышение уровня защищенности веб-приложений	Веб-приложения (O_2)	– Предоставить возможность авторизованному пользователю завершать сессию работы в приложении, а также гарантированно удалять идентификатор сессии по её завершению. – Для доступа к защищенным ресурсам веб-приложения требуется аутентификация пользователя на основе хранения аутентификационных данных только в криптографически защищенном виде. Данные не должны храниться в файлах и HTML-страницах, доступных по URL, а также информации, позволяющей делать выводы о структуре каталогов веб-приложения на сервере. – Если пользователь может вносить изменения в свой профиль, требуется подтверждение дополнительной процедурой аутентификации. – Необходимо осуществлять фильтрацию входного потока данных для предотвращения использования опасных HTML-тегов. – В случае ошибки в приложении необходимо запретить доступ к данным о структуре файловой системы и SQL-выражениям, используемым при доступе к базе данных. Вместо этого следует выдавать пользователю страницу-заглушку с кодом HTTP-ответа веб-сервера «200». – При прохождении процедуры аутентификации необходимо использовать защищенные протоколы Kerberos или TLS v1.2 (и выше) и передачу аутентификационных данных следует осуществлять методом POST.

Продолжение табл. 13

		– Необходимо исключить использование данных в формате XML внешних сущностей, внешних параметров сущностей и внешних описаний типа документа при обработке веб-сервером. – Запретить кеширование веб-форм ввода конфиденциальной информации и выставить атрибут HTTPOnly у параметров cookie, значения которых не должны быть доступны сценариям, выполняемым браузером. Также необходимо выставить атрибут secure у параметров cookie, содержащих чувствительную информацию. – Необходимо проводить проверку корректности вводимых пользователем данных как на стороне клиента, так и на стороне сервера. – Использовать директивы в заголовках сообщений HTTP для определения применяемой кодировки и избежать использования разных кодировок для разных источников входных данных. – Проверять JavaScript-код, подгружаемый со сторонних ресурсов, на предмет вредоносного воздействия и возможность кражи аутентификационных данных и файлов-cookie пользователей. Также необходимо периодически проверять хэш-суммы используемых JavaScript и в случае изменения отключать использование JavaScript на сайте для выполнения повторной проверки функциональности. Отказаться от использования динамически формируемых кодов JavaScript на веб-ресурсе и отдавать предпочтение загрузке внешних зависимостей из контролируемых источников.
Обеспечение защиты беспроводной сети	Персональные мобильные устройства (O_5)	В организации должны использоваться следующие сегменты сети: 1) Гостевой сегмент, позволяющий использовать Интернет-ресурсы. Доступ к данному сегменту предоставляется третьим лицам, не являющимся работниками организации, которым необходим доступ в сеть Интернет; 2) Корпоративный сегмент, позволяющий использовать Интернет-ресурсы. Доступ к данному сегменту должен предоставляться по доменной учетной записи, после добавления учетной записи в специальную группу доступа. Доступ к данному сегменту предоставляется всем работникам, которым необходим доступ в сеть Интернет; 3) Доменный сегмент, используемый для корпоративных мобильных устройств, подключенных к домену, и позволяющий использовать Интернет-ресурсы, сетевые ресурсы организации, пользовательские интерфейсы внутренних веб-сервисов (без возможности администрирования). Доступ к данному сегменту должен предоставляться по доменной учетной записи, после

Окончание табл. 13

		после добавления учетной записи в специальную группу; 4) Привилегированный сегмент, позволяющий использовать Интернет-ресурсы, ресурсы сети передачи данных организации, сетевые ресурсы и информационные активы. Доступ к данному сегменту должен предоставляться по доменной учетной записи, после добавления учётной записи в специальную группу доступа; 5) Технологический сегмент для служебной необходимости работников управления информационных технологий организации, позволяющий использовать Интернет-ресурсы, ресурсы сети передачи данных, информационные активы организации. Доступ к данному сегменту должен предоставляться по доменной учетной записи, после добавления учетной записи в специальную группу доступа. – Доступ из гостевого и корпоративного сегментов беспроводной сети в сети передачи данных должен быть заблокирован. В организации должно быть запрещено подключение личных точек беспроводного доступа (Wi-Fi маршрутизаторов), к сети передачи данных, без согласования с управлением безопасности.

Таблица 14

Комплексная система мер и процедур, отвечающая за контроль выполнения требований, определенных частной политикой

Предложенные меры безопасности в рамках противодействия сетевой атаке на уровне приложений	Меры контроля
Применение программных платформ с автоматической проверкой и преобразованием данных пользователя, основанных на фреймворках	Проверка корректности работы фреймворков через тестирование на предмет уязвимостей
Применение метода проверки входных данных путем их сопоставления с заранее определенным списком допустимых значений	Регулярное обновление белых списков для добавления новых допустимых значений и удаления устаревших
Применение WAF (Web Application Firewall)	Мониторинг логов работы WAF для выявления атак и аномального поведения
Разделение данных, обрабатываемых, хранимых или передаваемых приложением на категории с целью определения информации, требующей дополнительной защиты, и дальнейшее ограничение доступа в соответствии с установленными классификациями	Надежное хранение и передача данных, обеспечивающие соответствие с установленными требованиями безопасности
Предоставление доступа к общедоступным ресурсам в стандартной конфигурации, при этом ограничивая доступ ко всем остальным ресурсам	Регулярное обновление списка общедоступных ресурсов для учета изменений в требованиях безопасности

Продолжение табл. 14

Регулирование доступа к моделям данных через назначение владельцев записей, а не путем установки прав пользователей на их создание, просмотр, обновление или удаление	Контроль доступа к данным на основе владельцев записей, с ограничением доступа только тем пользователям, которые являются владельцами конкретных записей
Запрет вывода списка каталогов веб-сервером и устранение возможности доступа к метаданным файлов (например, git) и файлам резервных копий в корневых каталогах веб-сайта	Регулярное обновление настроек сервера для предотвращения вывода списка каталогов и обеспечения отсутствия метаданных файлов и файлов резервных копий
Фиксирование событий, связанных с запретом доступа к ресурсам	Автоматическое оповещение администраторов о событиях запрета доступа
Установка ограничений на частоту доступа к API и веб-интерфейсу для снижения вероятности автоматизации атак	Ограничение частоты запросов и количества запросов с определенного IP-адреса или пользователя, чтобы предотвратить перегрузку сервера и другие виды атак
Применение методов проверки типов данных и допустимых значений входных параметров	Использование механизмов проверки типов и допустимых значений входных данных для предотвращения ошибок программирования, а также для защиты от уязвимостей, связанных с неверными входными данными или введением вредоносного кода

Также общему снижению рисков способствует повышение грамотности сотрудников в сфере безопасности информации.

Вышеуказанные меры защиты позволят значительно снизить риск реализации векторов атак, приведенных в табл. 1.

Заключение

Подводя итог всему выше сказанному, можно предложить несколько основных способов реализации защиты информации от атак на уровне приложений:

- внедрение уже существующих систем защиты информации или разработка собственных, соответствующих российским и международным стандартам,
- использование в рамках КС актуального ПО,
- контроль за протекающим внутри КС трафиком информации,
- разработка, с учетом опыта компаний, стандартов реализации КС, отвечающих требованиям конкретных предприятий,
- разработка частных политик безопасности информации с учетом всех сфер деятельности различных организаций,
- ознакомление и изучение исследований в области защиты информации.

Соблюдение всех вышеуказанных мер поможет существенно сократить риск успешной атаки на уровне приложений. А также значительно повысит безопасность объектов КС и объектов критической инфраструктуры.

Список литературы

1. Моделирование векторов атак. URL: https://antihacking.ru/vectors (дата обращения 27.04.2023).

2. Эволюция атак на веб-приложения. URL: https://habr.com/ru/articles/334054/ (дата обращения 27.04.2023).

3. Common Attack Pattern Enumeration and Classification. URL: https://capec.mitre.org (дата обращения 27.04.2023).

4. DataSet UNSW-NB15. URL: https://www.kaggle.com/datasets/alextamboli/unsw-nb15 (дата обращения 27.04.2023).

5. Уязвимости и угрозы веб-приложений в 2020-2021 гг. URL: https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020-2021/ (дата обращения 27.04.2023).

6. Common Weakness Enumeration. URL: https://cwe.mitre.org/index.html (дата обращения 27.04.2023).

7. Статистика уязвимостей веб-приложений в 2018 году. URL: https://www.ptsecurity.com/ru-ru/research/analytics/web-application-vulnerabilities-statistics-2019/ (дата обращения 27.04.2023).

8. БДУ ФСТЭК России URL: https://bdu.fstec.ru/vul (дата обращения 27.04.2023).

9. Стандарты в области информационной безопасности. URL: https://www.altell.ru/legislation/standards/ (дата обращения 27.04.2023).

10. ISO/IEC 27001. Системы менеджмента информационной безопасности. URL: https://www.iso.org/ru/standard/27001 (дата обращения 27.04.2023).

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 03.05.2023

Информация об авторах

Хромых Сергей Алексеевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Остапенко Григорий Александрович – д-р техн. наук, проректор Финансового университета при Правительстве Российской Федерации, e-mail: alexanderostapenkoias@gmail.com

Щербакова Дарья Владимировна – соискатель, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

Остапенко Александр Алексеевич – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

NETWORK ATTACKS AT THE APPLICATION LEVEL: RISK LANDSCAPE AND PRIVATE INFORMATION SECURITY POLICY OF THE ENTERPRISE

S.A. Khromykh, G.A. Ostapenko, D.V. Shcherbakova, A.A. Ostapenko

The problem of network attacks at the application level is considered and its relevance to this problem is substantiated. Vectors and vulnerabilities of network attacks at the application level are given. A risk assessment methodology based on data on attacks and vulnerabilities in 2022 is described and implemented. A vulnerability matrix and a risk landscape are built based on risk assessment data in the specified period. Based on the risk landscape, the degree of danger of attack vectors and vulnerabilities is assessed. The most dangerous combinations of vectors and vulnerabilities are highlighted. For such combinations, corresponding fragments of a private information protection policy are proposed. Attention is focused on the importance of developing private information security policies that take into account the specifics of the activities of specific enterprises for more effective protection against attacks at the application level and beyond.

Keywords: attack vectors, vulnerabilities, risk landscape, private policy.

Submitted 03.05.2023

Information about the authors

Sergey A. Khromykh – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Grigory A. Ostapenko – Dr. Sc. (Technical), Vice-Rector of the Financial University under the Government of the Russian Federation, e-mail: alexanderostapenkoias@gmail.com

Darya V. Shcherbakova – applicant, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com

Aleksandr A. Ostapenko – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com